Virtualization from the Desktop to the Data Center p. 67

Windows® IT Pro

A PENTON PUBLICATION

MAY 2011 | WINDOWSITPRO.COM | WE'RE IN IT WITH YOU

Use > Windows Intune to manage PCs from the cloud p. 23

Mark Russinovich on Windows Azure p. 29

Active Directory Disaster Recovery p. 33

Deciphering PKI p. 37

Exchange 2010 Auditing Administrator Actions p. 41

Deploy FAST Search Server 2010 for SharePoint p. 47

Exchange Server Client Access p. 53

Netezza. Up and running in 24 hours, not 24 days.

Get set up in hours instead of days, and start counting returns in minutes instead of hours. All with IBM's Netezza data warehouse appliance for high-performance analytics. It gives you analytics reports at supersonic speeds. At a fraction of the cost of Oracle Exadata. Get real, actionable business results fast.

ibm.com/facts

COST comparison based on publicly available information as of 2/10/2011 for an Oracle Exadata X2-2 HP Full Rack and a full rack of Netezza TwinFin. The cost to acquire Netezza can be as low as 1/6 of Exadata if a client is acquiring new Oracle database licenses and as low as 1/2 if using existing Oracle database licenses. IBM, the IBM logo, ibm.com, Smarter Planet and the planet icon are trademarks of International Business Machines Corp, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at www.ibm.com/legal/copytrade.shtml.

CONTENTS

COVER STORY

FEATURES

INTERACT

IN EVERY ISSUE

Access articles online at www.windowsitpro.com. Enter the article ID (located at the end of each article) in the InstantDoc ID text box on the home page.

Windows IT Pro
A PENTON PUBLICATION
MAY 2011
VOLUME_17 NO_5

COLUMNS

CONTENTS

PRODUCTS

Windows IT Pro

EDITORIAL

Editorial and Custom Strategy Director
Michele Crockett mcrockett@windowsitpro.com

Editor in Chief
Amy Eisenberg amy@windowsitpro.com

Senior Technical Director
Michael Otey motey@windowsitpro.com

Technical Director
Sean Deuby sdeuby@windowsitpro.com

Senior Technical Analyst
Paul Thurrott news@windowsitpro.com

Industry News Analyst
Jeff James jjames@windowsitpro.com

Custom Group Editorial Director
Dave Bernard dbernard@windowsitpro.com

Developer Content
Anne Grubb agrubb@windowsitpro.com

Exchange & Outlook
Brian Winstead bwinstead@windowsitpro.com

Networking, Storage, Hardware
Jason Bovberg jbovberg@windowsitpro.com

SharePoint
Caroline Marwitz cmarwitz@windowsitpro.com

SQL Server
Megan Keller mkeller@windowsitpro.com

Systems Management, Virtualization, Windows OS
Zac Wiggy zwiggy@windowsitpro.com

Editorial Web Architect
Brian Reinholz breinholz@windowsitpro.com

CONTRIBUTORS

SharePoint and Office Community Editor
Dan Holme danh@intelliem.com

Senior Contributing Editors
David Chernicoff david@windowsitpro.com
Mark Joseph Edwards mje@windowsitpro.com
Kathy Ivens kivens@windowsitpro.com
Mark Minasi mark@minasi.com
Paul Robichaux paul@robichaux.net
Mark Russinovich mark@sysinternals.com

Contributing Editors
Alex K. Angelopoulos aka@mvps.org
Sean Deuby sdeuby@windowsitpro.com
Michael Dragone mike@mikerochip.com
Jeff Fellinge jeff@blackstatic.com
Brett Hill brett@iisanswers.com
Darren Mar-Elia dmarelia@windowsitpro.com
Tony Redmond 12knocksinna@gmail.com
Ed Roth eroth@windowsitpro.com
Eric B. Rux ericbrux@whshelp.com
John Savill john@savilltech.com
William Sheldon bsheldon@interknowlogy.com
Randy Franklin Smith rsmith@montereytechgroup.com
Curt Spanburgh cspanburgh@scg.net
Orin Thomas orin@windowsitpro.com
Douglas Toombs help@toombs.us
Ethan Wilansky ewilansky@windowsitpro.com

ART & PRODUCTION

Production Director
Linda Kirchgesler linda@windowsitpro.com

Senior Graphic Designer
Matt Wiebe matt.wiebe@penton.com

ADVERTISING SALES

Publisher
Peg Miller pmiller@windowsitpro.com

Business Development Director
Kerry Gates kerry.gates@penton.com

EMEA Managing Director
Irene Clapham irene.clapham@penton.com

Director of IT Strategy and Partner Alliances
Birdie J. Ghiglione birdie.ghiglione@penton.com 619-442-4064

Online Sales and Marketing Manager
Dina Baird Dina.Baird@penton.com

Key Account Director
Chrissy Ferraro christina.ferraro@penton.com 970-203-2883

Account Executives
Barbara Ritter barbara.ritter@penton.com 858-367-8058
Cass Schulz cassandra.schulz@penton.com 858-357-7649

Client Project Managers
Michelle Andrews 970-613-4964
Kim Eck 970-203-2953

Ad Production Supervisor
Glenda Vaught glenda.vaught@penton.com

MARKETING & CIRCULATION

Customer Service service@windowsitpro.com

IT Group Audience Development Director
Marie Evans marie.evans@penton.com

Marketing Director
Sandy Lang sandy.lang@penton.com

CORPORATE

PENTON

Chief Executive Officer
Sharon Rowlands Sharon.Rowlands@penton.com

Chief Financial Officer/Executive Vice President
Nicola Allais Nicola.Allais@penton.com

TECHNOLOGY GROUP

Senior Vice President, Technology Media Group
Kim Paulsen kpaulsen@windowsitpro.com

WRITING FOR *WINDOWS IT PRO*
Submit queries about topics of importance to Windows managers and systems administrators to articles@windowsitpro.com.

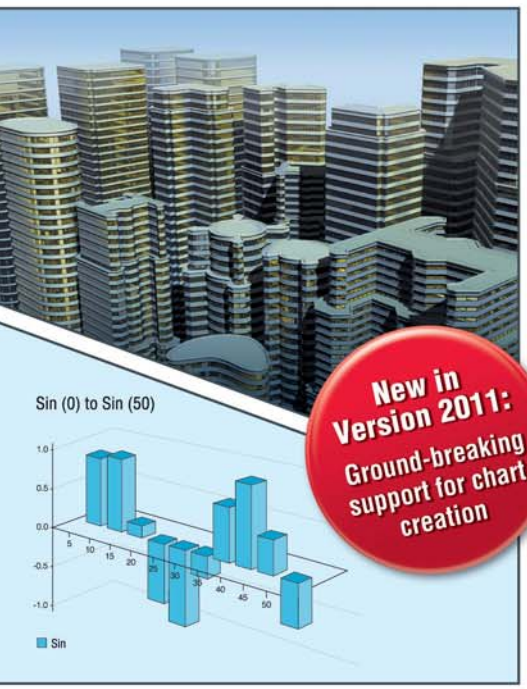
LIST RENTALS
Contact MeritDirect, 333 Westchester Avenue, White Plains, NY or www.meritdirect.com/penton.

REPRINTS
Diane Madzelonka, Diane.madzelonka@penton.com, 216-931-9268, 888-858-8851

Create cutting edge reports with the complete set of tools from Altova®

ALTOVA® missionkit®

Experience how the Altova MissionKit®, the integrated suite of XML, database, and data integration tools, lets you display and analyze data through enhanced chart and report generation.



Report generation is finally easy – and affordable – with Altova MissionKit reporting tools:

StyleVision® – stylesheet and report design tool

- Consolidated reporting based on XML, database and/or XBRL data
- Dynamic data selection and rendering
- HTML, Microsoft Word, PDF, and e-Form report creation

XMLSpy® – advanced XML editor

- Instant creation of charts to analyze XML data
- One-click export of charts to XSLT, XQuery, or image files

MapForce® – any-to-any data mapping tool

- Integration with StyleVision for rendering attractive reports
- Report generation for virtually any data format: XML, databases, EDI, flat files, Excel 2007+, and more

Download a 30 day free trial!

Try before you buy with a free, fully functional, trial from

www.altova.com

Crockett

"Your ability and willingness to facilitate, if not drive, the platform selection process affect not only your organization's success but your own career."

Embracing the Next Platform Change

Are you ready for the new database, cloud computing, or mobile computing platform?

Depending on your tolerance for change, career preparation, and sense of adventure, contemplating any sort of software platform switch will evoke in you gleeful anticipation or abject dread—or, most likely, some combination of the two. Regardless of how you feel about change, you likely have been or will be involved in a platform selection and deployment process. As businesses constantly look for ways to improve processes, reduce costs, and increase efficiency—ultimately, to boost profitability and market share—the IT platforms that run the business are perpetually under review.

Your ability and willingness to facilitate, if not drive, the platform selection process affect not only your organization's success but your own career. Are you dragged into platform changes kicking and screaming? Do you wait until the decision is made, then smile and roll up your sleeves for the deployment phase? Or do you notice that business systems could be better, research alternatives, sell the solution to your managers, and drive the change process?

Although cloud computing and mobile development platform choices are trendy topics, examining the database platform selection process reveals the classic battle among opposing forces: a tendency toward preserving the status quo among IT professionals who have invested their careers in learning a specific skill set, the business need to consolidate disparate database systems, and a reluctance on the part of both company leaders and IT departments to tamper with systems that could bring the business to a halt.

Despite the complications and potential risk, database platform switches and cross-platform implementations are on the rise. The *Windows IT Pro* audience has historically represented a cross-section of database adoption: About 54 percent of readers use SQL Server, about 18 percent use Oracle, and about 20 percent use MySQL, according to an independent Readex audience profile conducted in 2009.

Raj Gill, founder and CTO of Dallas-based Scalability Experts, said that database platform switches are driven by the typical factors of cost savings, standardization, and operational and management efficiencies. Particularly when companies are formed through a series of mergers and acquisitions, managing disparate databases can be difficult and expensive.

"The sheer cost of managing a variety of database platforms can be daunting," Gill said. "Consolidation across multiple database platforms does not work very well. So the first step for an organization would be to standardize on a couple of database platforms and then migrate—consolidating within each type."

Migration tools such as Microsoft's SQL Server Migration Assistant (SSMA) can help organizations plan a smooth transition. Gill noted that a company's success with the tool depends on a couple of factors.

"If the business logic is primarily sitting in the database object, then SSMA works well," he said. "But if the business logic is embedded in the application layer, then the migration assessment can become more involved." Gill said that Scalability Experts has built a toolset to "automate all scenarios of migrations to quickly arrive at the cost and effort to migrate very complex applications."

The availability of appropriate skill sets is a critical factor in the success of a database platform switch, according to Gill. "Two or three database platforms are common in a typical company," Gill said. "If DBAs can support multiple database platforms, they are automatically in high demand. Right now, the combination of Oracle and SQL Server skills is hot."

Scalability Experts has written coursework called *Practical SQL Server (PRASS) for Oracle DBAs* (www.scalabilityexperts.com). For another perspective on transferring database platform skills, you can follow well-known Oracle expert Jonathan Lewis as he chronicles his experiences adapting his general database expertise to SQL Server in his Simple-Talk blog series (www.simple-talk.com/sql/learn-sql-server/oracle-to-sql-server-crossing-the-great-divide,-part-1/).

"At the end of the day, companies need a highly skilled team to manage mission-critical systems," Gill said. "Cross training and functional readiness are key."

To boost your ability to manage mission-critical databases, consider becoming a Microsoft Certified Master (MCM) on SQL Server (www.microsoft.com/learning/en/us/certification/master-sql-path.aspx). If you'd like more perspective on adapting your skill set to meet the trends toward multi-platform computing, check out the Professional Career Development Seminar that we're producing in cooperation with Microsoft at Tech•Ed 2011 in Atlanta on May 15 (northamerica.msteched.com/topic/details/PRC100). *Windows IT Pro* experts Michael Otey, Sean Deuby, Paul Thurrott, and Richard Campbell will moderate panel discussions that will help you navigate IT career choices of the future—regardless of the next best platform.

InstantDoc ID 129954

MICHELE CROCKETT (michele.crockett@penton.com) is editorial strategy director of Penton Media's IT and developer publications, including *DevProConnections*, *Windows IT Pro*, *SharePoint Pro*, *SQL Server Magazine*, and *Connected Planet*.

James

"All of these trends have the potential to disrupt your IT operations if they're not handled proactively."

Choosing a New IT Platform

Weigh the variables before you deploy

One of the most important projects any IT department can undertake is the selection of a new IT platform. I'm not talking about adding minor software packages or modest hardware additions. I'm getting at the sprawling, enterprise-wide deployments that have the potential to generate significant rewards in terms of reduced IT costs, efficiency, and IT agility, while simultaneously threatening to throw your operations into chaos, bring work to a halt, and drain your IT resources.

Deployments that fall into this category include adopting Hyper-V or VMware to virtualize most of your server infrastructure, choosing between Office 365 and Google Apps/Mail, choosing a cloud platform to offload a vital business process, or deploying SharePoint across multiple branch offices and physical locations.

If you're considering radical upgrades to your IT environment along these lines, you aren't alone: IT research firm Enterprise Strategy Group (ESG) recently revealed that more than 60 percent of midsized-to-large enterprises plan to boost their virtualization spending in 2011 ("2011 Virtualization Software Spending Trends," bit.ly/i3vaLK).

Research giant Gartner recently released a list of 10 top technology trends for 2011 (bit.ly/af53gO) that it classified as strategic technologies with the "potential for significant impact on the enterprise in the next three years....[including] a high potential for disruption to IT or the business, the need for a major dollar investment, or the risk of being late to adopt."

Chief among those trends are cloud computing, mobile apps and tablets, social communications and collaboration, and next generation analytics. All of these trends have the potential to disrupt your IT operations if not handled proactively. So what is the best way to deploy new technology and platforms?

Do Your Homework

To get some advice on the subject, I spoke with Douglas Toombs, a *Windows IT Pro* contributing editor and senior analyst for managed services and cloud computing at Tier 1 Research. Toombs suggests that IT leaders should be cautious about jumping onto any platform bandwagon before a full risk assessment is done.

In the case of cloud computing, Toombs listed a number of potential pitfalls that IT leaders should be aware of. "There are lots of issues that need to be addressed before moving any of your IT infrastructure to the cloud," Toombs said. "Things like source-code escrow agreements are mechanisms by which organizations mitigate against future risk of a software vendor going out of business. In that circumstance, you still have the data on your own servers, and the software usually will still be usable for quite some time—probably enough time to find an alternate solution or engage the source-code escrow clause. With a [cloud] service provider, especially SaaS, they have it all. They have the software, the servers, and your data. This requires organizations to consider different mitigation strategies to protect themselves against the future risk of a service provider going out of business."

Toombs also pointed to server virtualization platforms, with IT pros commonly deciding between VMware and Microsoft server virtualization offerings. Both vendors take slightly different approaches to virtualization, especially when it comes to the cloud. Knowing the strengths and weaknesses of both approaches is vital, especially when it comes to connecting your internal, private clouds with services offered by external cloud providers.

"If you've already decided on VMware for your virtualization stack, moving to the cloud will be made easier by using VMware's vCloud Director product, which connects virtualization to the cloud orchestration layer used by VMware vCloud partners like Verizon, Terremark, and BlueLock," says Toombs. "There aren't as many Hyper-V-based cloud providers in the United States, but there are some in Europe."

Good Advice, Regardless of Platform

A report by Forrester Research's Philipp Karcher, "Pitfalls to Avoid When Upgrading to Microsoft Office 2010," bit.ly/hZ2Dir, points out some problems to avoid, but also provides some valuable advice for all large IT platform deployments.

"Upgrading Microsoft Office can prove daunting, especially for firms still on Microsoft Office 2003 or previous versions," Karcher said. "Although Windows 7 upgrades and hardware refreshes will accelerate the transition, buyers remain wary of business disruptions, ranging from compatibility issues to the transition to a new user interface. The recipe for a successful Office upgrade includes a heavy dose of planning, an ample amount of input from the business, a package of training, and just the right amount of remediation to minimize risk."

Have you gone through some big IT platform rollouts of your own? Send your advice and suggestions to me via email at jeff.james@penton.com, and/or follow me on Twitter @jeffjames3.

InstantDoc ID 129956

JEFF JAMES (jeff.james@penton.com) is industry news analyst for *Windows IT Pro*. He was previously editor in chief of Microsoft TechNet magazine.

LETTERS@WINDOWSITPRO.COM

Spiceworks Review

I read Michael Dragone's review of Spiceworks 4.5 (InstantDoc ID 125235), and I'm wondering whether anyone has performed a security analysis on the software—I'm always skeptical of free software. One of our administrators installed the tool without permission and entered in the Domain Administrator account, so I'm a little concerned. Any suggestions?

—Brent W

I'm not aware of anyone having done a penetration test or code review of Spiceworks, nor have I come across anyone who has done a packet trace on a machine running Spiceworks. That would be my suggestion: Use Microsoft's Network Monitor or a similar tool and capture the packets that Spiceworks sends and receives in a lab environment. Of course, in your case, it's too late for that, so it would be a good idea at this point—if you're still feeling uncomfortable—to change your Domain Administrator account password (if you haven't already). The downside to this is that Spiceworks sends and receives packets to the Internet over SSL, so you'd only see encrypted payloads sent to and from them.

The Spiceworks privacy policy (www.spiceworks.com/privacy) states that the inventory data collected is stored locally and not transmitted to Spiceworks and that the company doesn't resell customer data. Personally, I don't believe Spiceworks was written with any malicious intent, but I agree with your wariness and certainly appreciate your concerns.

—*Michael Dragone*

Frustration with Windows Phone 7

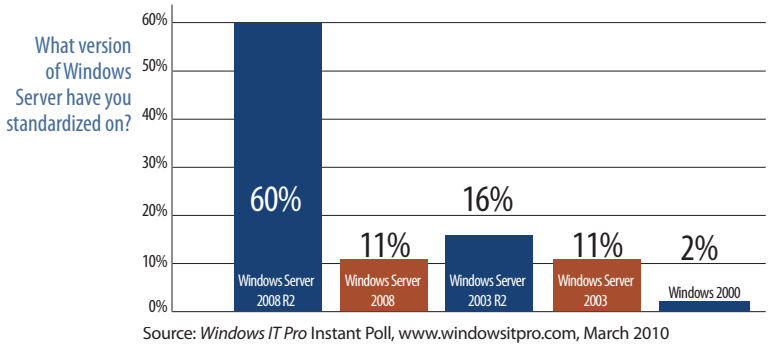
I read Paul Thurrott's Short Takes article, "Microsoft Sort of Admits Carriers Have Delayed the First Windows Phone Update(s)" (InstantDoc ID 129871) and listened to his *Windows Weekly* podcast dated March 10th (http://twit.tv/ww199). His frustration with Microsoft over the Windows Phone 7 updates is clearly evident and justified. These days, when *Wag the Dog* seems to be the law of the land, it's good to see Paul with the fervor to hold Microsoft's feet to the fire. I delayed purchasing my first smartphone, awaiting the delivery of Windows Phone 7. I finally tired of waiting and purchased a Droid X. As things have turned out, I'm very glad that I did. I might try a Windows Phone 7 device one day, but not anytime soon.

Thanks for the high-quality journalism, the intelligence, and (yes) the entertainment value you bring to the *Windows Weekly* podcast. Just hang in there—I'm sure I'm not the only person disgusted with Microsoft's handling of this phone situation.

—Chuck Johns

InstantDoc ID 129951

Instant Poll Results: Windows Server



Source: *Windows IT Pro* Instant Poll, www.windowsitpro.com, March 2010

Windows IT Pro welcomes feedback about the magazine. Send comments to letters@windowsitpro.com, and include your full name, email address, and daytime phone number. We edit all letters and replies for style, length, and clarity.

Thurrott

"With iPads getting more powerful and PCs picking up some iPad-like simplicity cues, the only thing clear about the future is that the iPad has changed everything."

Windows Phone's Lack of Updates, Android vs. the iPhone, and Apple iPad Domination

The year's barely one-quarter done, and I'm already shocked by the rapid change that's sweeping our industry. I can't predict exactly what's going to happen for the rest of 2011, but I can tell you this: Things are going to be pretty different when we get to the other side.

Is Windows Phone Failing?

Microsoft launched Windows Phone 7 last year with some fanfare and perhaps a bit too much self-congratulation. Windows Phone does offer innovative features such as hubs and live tiles, and a more natural and elegant UI than the Android and iPhone market leaders. But just being better isn't enough in this market. Since the launch, the Windows Phone team has publicly stated, repeatedly, how impressed it is with itself for moving so quickly. There's just one problem: Windows Phone didn't get a single software update for over five months.

What's five months? Nothing, if you're talking about a 2003-era feature phone, or any phone that shipped before the iPhone. But in 2011, five months is the difference between life and death. After all, why should customers care about Windows Phone if Microsoft doesn't?

In Microsoft's rush to market, it delivered the initial Windows Phone 7 OS in an incomplete and, it should be admitted, buggy state. And the unspoken promise was that this was acceptable only because Microsoft would move to fix the bugs, and add new features very quickly.

While Apple was able to ship five software updates—with some major new features, mind you—for its own far more stable and more mature iPhone between the Windows Phone launch and its first update, Microsoft was busy fending off (true) claims that its carrier partners could block software updates for one update cycle. Actually, it's not clear what it was busy doing. It appears to have done nothing at all.

Unless something changes, Microsoft will ship one more software update for Windows Phone in 2011. Code-named Mango, it's a major update, with new features like Internet Explorer 9, multi-tasking for third-party apps, background audio playback for third-party apps, background downloading, and more. Apple will have delivered several more iPhone software updates, and a major iPhone hardware revision by then.

There are two signs of hope. First, Nokia will be putting its full weight behind Windows Phone, and while we won't really see the effects of this influence until 2012, the company has a wide enough reach that it could actually make a difference. Second, the Windows Phone team recently gained a new hire who, I'm told, will turn things around for software updates. If this is true, perhaps Windows Phone will be updated at least quarterly. This seems like a bare minimum to me, given how fast the competition is moving.

I'm still upbeat about Windows Phone from a technical perspective, but I'm not so positive about its chances in the market. I've written before about the uncertainty around how many phone platforms the market can handle. Microsoft better hope it's a big number.

Android is Beating the iPhone

While Microsoft is joining a group of also-rans in the smart phone market, two platforms stand out: Google's Android and Apple's iPhone. Comparisons have been made between this market battle and the earlier PC vs. Mac wars, and I think that's valid. In the same way that the insular and consistent Mac market was overrun by the PC hordes, the iPhone has already been edged out of the top spot by a mess of Android handsets. And the gap is only growing.

What we see for the next year or two is clear: Android is the market leader and iPhone moves into the number two spot. (Current players like RIM Blackberry and Nokia appear to be on the way out.) I don't feel either platform offers the best all-around scenario for users—and neither rises in any way to the superior Windows Phone UI—but I have to give the iPhone the nod here.

One reason is that Android is a mess. There are far too many Android handsets, many of which are updated on a Windows Phone-esque schedule, seriously fragmenting the market for these devices and creating a nightmare of intersecting features between the different phones. As well, various aspects of the Android experience are decidedly lackluster, especially the Android Market, which bears more resemblance to a street market selling illegal goods than it does to a legitimate e-store. It's an embarrassment.

Another reason is that iPhone offers the cleanest experience, and the biggest ecosystem. iPhone offers many more apps, and it's also got the best selection of movies, TV shows, podcasts, books, and e-learning content of any smart phone platform.

Both Android and iPhone support important enterprise standards, especially Exchange Active Sync, so the real difference comes down to choice (Android) vs. ecosystem (iPhone). So far, Android

is winning. But iPhone gets my vote for the superior smart phone platform this year.

iPad Owns the Tablet Market

While we're discussing the superior Apple smart phone platform, it makes sense to glance at the iPad 2, Apple's latest entry in a market it created single-handedly last year. We call them tablets. But we might as well just call them iPads, because in this market, there's iPad and then there's everything else. And everything else isn't all that compelling.

Apple sold about 14 million iPads over nine quarters in 2010, which wasn't too shabby, though it was a far cry from the 350 million PCs that hardware makers sold that year. In 2011, all tablet makers are expected to sell a whopping 52 million devices, however, and almost 75 percent of those, or about 37 million of them, will be iPads.

Consumers are picking simplicity over power in ever-increasing numbers. Analysts have already cut their initial 2011 PC sales estimates because of this shift.

And as with the iPhone before it, the iPad is seeing a very rapid uptick in businesses of all sizes. Which makes sense, since most people simply need to access email and the web, and let's face it, the iPad is lighter, smaller, and gets better battery life than almost any portable PC around. Granted, certain users will always need a keyboard, and for them a PC (or, gasp, a Mac) will still be the better option.

But as iPads and PCs converge—with iPads getting more powerful and PCs picking up some iPad-like simplicity cues—the only thing that's clear about the future is that the iPad has changed everything. You've been warned.

Alternative Platforms as a Choice

Even the most diehard of Windows shops has seen the trends: First users wanted the BlackBerry, but now they're clamoring for Android phones and iPhones, iPads and Macs.

What we used to call alternative platforms—that is, non-Microsoft platforms—are everywhere. It's too bad Linux couldn't have been invented this year: It would have been a smash hit.

We see this trend in other places too. HP says it will ship all of its PCs with Windows and Palm webOS by 2012, letting customers dual-boot between the two, and the company is prepping a webOS-based tablet that will compete with the iPad.

RIM, too, is in the tablet game with its PlayBook. Google is offering a PC OS called Chrome OS that's based on its web browser and threatens Windows.

Microsoft is so freaked by all this that it's moving its dominant product, Windows, to new markets and form factors with Windows 8, due in 2012.

What we used to call alternative platforms—that is, non-Microsoft platforms—are everywhere. It's too bad Linux couldn't have been invented this year: It would have been a smash hit.

I think we're going to see core markets, like mainstream computing, the web, and smart phones, all served by multiple players. Microsoft will continue as a player, but it won't be the dominant force in any of these markets.

It's the Hardware

Someday, we'll look back and explain how this change happened, and it will seem as inevitable then as it seems confusing today. I don't profess to have all of the answers, but I think part of the explanation lies with the hardware.

We spent years in the tech industry operating under the auspices of Moore's Law, in which, roughly speaking, computing power doubles every 18 months. (That's not what Moore's Law really says. But that's basically what it means.)

Moore's Law is as convenient a premise for the tech industry as is Asimov's Law of Robotics for science fiction, and we have collectively spent much of the past few decades casually contorting our history to ensure it meshes.

But I've played 3D action shooters on an iPhone that would task a gaming PC from just a few years ago. We're not just beating Moore's Law. We're making it look silly.

That's because technology is about more than the number of transistors on a die, in the same way that it's about more than just the CPU in your PC. Our computing devices aren't just smarter, they're smaller, lighter, and portable, and they get incredible battery life.

You could almost fly from Boston to London and back and never sap an iPad's battery, and if you did it with the new crop of ThinkPads running Intel's latest iCore series of chipsets, you'd have hours of life left over. That's not just a game changer, it's a life changer.

Intel's new processors are fascinating, powerful stuff, a last minute recall-inducing bug notwithstanding. Other trends will have equally powerful effects on our computing experiences: With its iPad and MacBook Air machines, Apple has switched entirely to solid state storage, enabling it to build supernaturally thin devices with superior battery life. (And the Air does that with a two-generation-old Intel chipset, by the way.)

But you don't have to buy a new device to take advantage of this trend. Solid State Storage (SSD) disks can be added to existing PCs, replacing slower and less energy-efficient hard drives.

I'm in the middle of migrating all of my PCs to SSD, and while the drives are still expensive compared to traditional hard drives, the performance difference is likewise incredible.

Now if Apple could only invent an iPad screen that wasn't as reflective as my shaving mirror, maybe I'd be able to bite the bullet and enter this brave new world with a truly new device. Maybe.

InstantDoc ID 129970

PAUL THURROTT (thurrott@windowsitpro.com) is the senior technical analyst for *Windows IT Pro*. He writes a weekly editorial for *Windows IT Pro UPDATE* (www.windowsitpro.com/email) and a daily Windows news and information newsletter called *WinInfo Daily UPDATE* (www.wininformant.com).

Are you overpaying for Oracle Database? Hint: you're overpaying for Oracle Database.

The first thing to consider when thinking about DB2® for your business: it's as low as 1/3 the cost of Oracle Database. Then consider DB2 on Power Systems™ with 3x the performance per core of Oracle Database on SPARC, in TPC-C and SAP SD benchmarks. Overall, an ironclad case for IBM. There's more where that came from, too.

ibm.com/facts

THE CONVERSATION BEGINS HERE

Microsoft® Visual Studio® CONNECTIONS

Microsoft® ASP.net CONNECTIONS

Microsoft® Silverlight® CONNECTIONS

SharePoint CONNECTIONS

SQL Server CONNECTIONS

BONUS: *Cloud & Mobile App sessions*

Exchange CONNECTIONS

WINDOWS CONNECTIONS

UNIFIED COMMUNICATIONS CONNECTIONS

Karlsruhe Germany | **9-10 June 2011** | 8 June Workshops

London, UK | **14-15 June, 2011** | 13 June Workshops

DEVELOPERS • IT PROS • IT MANAGERS

- Train with 50+ Microsoft and industry experts at over 115 deep dive sessions
- Attend cutting edge keynotes and keep your competitive edge
- Network with speakers, partners and colleagues
- Attend the co-located event sessions at **no extra charge**

KEYNOTE SPEAKERS

STEVE FOX
Microsoft
Director, Developer and Platfrom Evangelism for SharePoint

DAVE MENDLEN
Microsoft
Senior Director Developer Platform and Tools

SCOTT GUTHRIE
Microsoft
Corporate Vice President .NET Developer Platform

TONY REDMOND
Tony Redmond and Associates

Providing the vision and intelligence to keep you and your company competitive in today's market!

A SAMPLING OF OUR INDUSTRY EXPERTS

DAN HOLME
Intelliem, Inc.

WOUTER VAN VUGT
code-counsel

JUVAL LOWY
IDesign, Inc.

DINO ESPOSITO
IDesign Inc.

SCOT HILLIER
Scot Hillier Technical Solutions, LLC.

STEFFEN KRAUSE
Microsoft Deutschland GmbH

DANIEL MELANCHTHON
Microsoft Deutschland GmbH

AGNES MOLNAR
BA Insight

REINER GANSER
Ganser IT-Consulting

BILLY HOLLIS
Author

NENO LOJE
www.teamsystempro.com

PETER MONADJEMI
activetraining

JOHN PAPA
Microsoft

PAUL S. RANDAL
SQLskills.com

KIMBERLY L. TRIPP
SQLskills.com

CHRISTIAN WENZ
Arrabiata Solutions GmbH

Check the Web site for the full list of sessions and speakers

QUESTIONS ANSWERED • STRATEGY DEFINED • RELATIONSHIPS BUILT

SPACE IS LIMITED Register Today! Call +44 (0)161 929 2800 |
www.DevConnections.com/Germany | www.DevConnections.com/UK

POWERED BY MICROSOFT, DEVCONNECTIONS AND ITCONNECTIONS

Minasi

"Windows PE's purpose is solely as a sort of 'starter OS' for maintenance, repair, and deployment."

Adding Windows PE to Your Windows 7 System

Install an "onboard emergency kit" OS on your hard disk—one built to be sleek and maintenance-focused

You're on the road, and you go to turn on your Windows box, but instead of booting, it hangs or bluescreens. You have an idea how to fix it, but how do you get the thing started in the first place to attempt the repair? If only you had a second OS on the hard disk—one built to be sleek and maintenance-focused, sort of an "onboard emergency kit." This month, I'll show you how to install such a kit. It may not sound like it, but this is an important component of the SteadyState discussion I began last month in "Replicating SteadyState in Windows 7" (InstantDoc ID 129192).

In case you've never heard of Windows Preinstallation Environment (WinPE), Microsoft gives it away as part of the Windows Automated Installation Kit (AIK). WinPE's purpose is solely as a sort of "starter OS" for maintenance, repair, and deployment. It's essentially Window 7 with the Start menu, most of its built-in tools, and virtually all the GUI removed—but that's ideal for your emergency needs. Directions for setting up WinPE on a CD or a USB stick are easy to find, but you need it installed permanently on the hard disk, and accomplishing that is somewhat trickier.

I've found three ways to put WinPE on a system. Two of the methods are quite complex, so I'm going to show you the simplest approach and save the truly ugly (but sadly sometimes necessary) ones for the future. WinPE can't reside on the same volume as Window 7, so in this scenario you'll add WinPE to an already-working Windows 7 system in five steps:

1. Install the AIK—Download the AIK for Windows 7 from the Microsoft Download Center (www.microsoft.com/downloads) and install it on your computer. (Yes, the AIK is big, but you can uninstall it when you're done and get rid of all that stuff. Once you've downloaded the file—it's an ISO file—burn it to a disk, run the startcd.exe file, and choose Windows AIK Setup.)

2. Shrink the C drive by 1GB—Open Disk Management, right-click the C drive, choose *Shrink volume*, and shrink the C drive by 1,000MB. Once that's done, you'll have 1,000MB of unallocated space on your main drive.

3. Create a new volume in that 1GB—Right-click that drive, choose *New simple volume*, and let the wizard format the space and give it a drive letter. (I'll use "W" in this example.) Now you've got a home for WinPE.

4. Image WinPE onto that partition—The AIK delivers two WinPE images: a 64-bit one and a 32-bit one. Both are named winpe.wim, so be sure to use the right one for your architecture. The 64-bit one is in C:\Program Files\Windows AIK\Tools\PETools\amd64\winpe.wim, and the 32-bit one is in C:\Program Files\Windows AIK\Tools\PETools\x86\winpe.wim. Click Start, All Programs, Microsoft Windows AIK, then shift-right-click Deployment Tools Command Prompt, choosing *Run as Administrator* and clicking Yes to the User Account Control (UAC) prompt if necessary. For example, I did this on my 64-bit system:

```
C:\Program Files\Windows AIK\Tools\PETools>imagex /apply
  "C:\Program Files\Windows AIK\Tools\PETools\amd64\winpe
  .wim" 1 w:\ /verify
```

While typing that, I cheated and shift-right-clicked on the winpe .wim file to put its entire path and filename in my clipboard so that I could paste it into that ImageX invocation. You should, too.

5. Create a new OS boot entry so that Windows gives you the option to boot WinPE at boot time from drive W—You'll use the Bcdedit commands I examined in my boot-from-VHD discussions in past columns, so they should look familiar. First, you'll copy the current OS entry so that you've got a starting point:

```
bcdedit /copy {default} /d "Boot WinPE"
```

That returns a new, long GUID that you'll need to enter into the following three commands:

```
bcdedit /set {insert new guid} device partition=w:
bcdedit /set {insert new guid} osdevice partition=w:
bcdedit /set {insert new guid} detecthal yes
```

Then, just add one new command that you haven't met before to set a new parameter *winpe* to *yes*, signaling to Windows that you're booting a WinPE image:

```
bcdedit /set {insert new guid} winpe yes
```

Reboot, and you'll get the payoff: Boot Manager will contain a Boot WinPE option. Congrats! Your "emergency OS" is now installed, or at least installed *one* way. I'll show you another approach next month.

InstantDoc ID 129793

MARK MINASI (www.minasi.com/gethelp) is a senior contributing editor for *Windows IT Pro*, an MCSE, and the author of 25 books, including *Administering Windows Vista Security: The Big Surprises* (Sybex).

FREE Evaluation

Get Your Head Out of the Clouds

SPECTOR 360 Solves Real-World IT Problems

Monitor, **capture** and **analyze** all user activity across PCs, Macs, laptops, and the Internet.

- **Review All Electronic User Activity**
- **Identify Security Breaches**
- **Streamline Business Operations**
- **Manage Compliance and Audits**

SPECTOR 360®
Monitoring, Analysis, and Management Software

Download a 15-Day Evaluation Today

Spector360Eval.com

Questions? Call Toll-free: **1.877.344.1427**

Otey

"Without a doubt, the cloud service I use most often is Microsoft's SkyDrive, a super handy cloud-based storage service."

Free Cloud Services

Store data, secure passwords, send large files, and other common networking tasks

Cloud computing is being pushed heavily by today's software vendors. However, cloud computing and Internet-based services really aren't new. In fact, there are many different cloud services and web applications available today that are completely free. In this column, I'll tell you about ten free cloud services that you can begin using right away.

10 **Hotmail and Gmail**—Who doesn't take advantage of one of these super useful services? Microsoft's Hotmail and Google's Gmail accomplish essentially the same thing: They provide free web-based email. Hotmail allows attachments up to 10GB; Gmail allows attachments up to 20GB. You can sign up for Hotmail at www.hotmail.com, or you can pick Gmail at www.gmail.com.

9 **Windows Live Messenger**—A part of Microsoft's Windows Live suite, Windows Live Messenger lets you perform both text-based chatting through IM as well as one-to-one video chats if your computer has an attached webcam. You can get it at www.microsoft.com/downloads/en/details.aspx?FamilyID=C575A6C6-C8DC-45E1-9E97-E0A437A5B770. Windows Live Messenger requires a Windows Live account.

8 **YouSendIt**—YouSendIt is a website that lets you send files that are too big to send as email attachments. The free Lite version lets you send files as large as 100MB. The recipient gets an email notification with a link when the file is available for download. If you need to send larger files, there's a Pro edition that allows files up to 2GB. You can find YouSendIt at www.yousendit.com.

7 **LastPass**—Keeping track of all your online passwords is a daunting task. LastPass is a web application that securely stores all your Internet passwords and can automatically enter them on website logon forms. You'll find LastPass at lastpass.com.

6 **Windows Live Sync**—Windows Live Sync enables you to synchronize directories between multiple computer systems. This service is especially useful for syncing your desktop and laptop when you travel. Windows Live Sync requires you to install a component on your desktop. You can take advantage of Windows Live Sync by going to www.foldershare.com.

5 **icloud**—icloud essentially offers a free online computer with a virtual desktop. The desktop gives you online storage and a variety of utility applications, including a word processor, calendar, web browser, and an application development environment. You can learn more about icloud at www.icloud.com.

4 **Sysinternals**—It seems I can't write a guide to free tools without mentioning Sysinternals. Sysinternals is well-known for its locally installed administrative tools. However, the majority of the Sysinternals tools can be run directly off the Sysinternals website as cloud services: There's no need to install them locally. These tools provide all sorts of useful file, disk, networking, and system process utilities. You can find the cloud-based versions of the Sysinternals suite at live.sysinternals.com.

3 **Windows Live SkyDrive**—Without a doubt, the cloud service I use most often is Microsoft's SkyDrive. SkyDrive is a super handy cloud-based storage service that lets you store up to 25GB of data for free. SkyDrive provides an easy-to-use web interface that lets you create folders for storage as well as providing drag-and-drop file uploading. The only requirement for using SkyDrive is that you have a Windows Live account. You can find SkyDrive at www.skydrive.com. I should note that there are other free web storage sites, but I've been perfectly happy with SkyDrive

2 **Google Apps**—One of the most well-known set of cloud-based applications is Google Apps. The free version of Google Apps includes Gmail, Google Calendar, Google Sites, and Google Docs. As its name suggests, Google Calendar is a shared online calendar that lets you schedule and share appointments. Google Docs is a Microsoft Office competitor that lets you create documents, spreadsheets, drawings, and presentations, and Google Sites lets you build websites and wikis. You can find Google Apps at www.google.com/apps.

1 **Amazon Web Services**—To prompt you to get started using its web services, Amazon offers a free version of its Elastic Compute Cloud (EC2) web service, which is good for one year. This free service is the EC2 Micro Instance, which includes 750 hours of EC2, 10GB of Amazon Elastic Block Storage, 5GB of Amazon S3 storage, 30GB of Internet data transfer, and 25 Amazon SimpleDB hours. You can find out more about Amazon's free web services usage tier at aws.amazon.com/free.

InstantDoc ID 129837

MICHAEL OTEY (motey@windowsitpro.com) is senior technical director for *Windows IT Pro* and *SQL Server Magazine* and author of *Microsoft SQL Server 2008 New Features* (Osborne/McGraw-Hill).

Deuby

"In an environment the size of the federal government, the potential for savings is enormous simply because the scale is enormous."

The Federal Government Embraces the Cloud

You think *you* have problems moving from an asset-based infrastructure to a service-based infrastructure!

The next time you want to complain about the problems your company is facing while moving from a traditional asset-based IT infrastructure to a service-based cloud computing infrastructure, consider Vivek Kundra's situation. As the federal government's first CIO, he has the task of reducing the cost of his $80 billion IT budget while increasing its flexibility. And like every other CIO who wants to keep his or her job, he's been looking seriously at the advantages that cloud computing can provide. Unlike many other CIOs, however, he's commanding his organization to begin using the cloud in a big way.

Kundra keynoted the Federal Cloud Computing Strategy at the 2011 Cloud Security Alliance Summit in San Francisco. In his presentation, he detailed the many reasons the federal government needed to begin moving to this new model. First, because the government's computing requirements are (like everyone else's) growing dramatically, it has been building data centers at a mind-boggling pace. Keep in mind: This is an infrastructure that's parallel to the existing commercial infrastructure even though (in many cases) the government's needs are no different than those of commercial businesses.

In the past 10 years, the US government went from owning 432 data centers to almost 2,100 data centers—a five-fold increase. As a result, 30 percent of federal IT spending last year went straight to data center infrastructure. (As the federal government has expanded, most companies are moving in the other direction, consolidating their data centers. For example, IBM recently consolidated from about 200 data centers to 12!) In addition to the massive amount of overhead this kind of infrastructure creates, it absolutely stifles any kind of agility or innovation because there's so much fiscal, intellectual, and emotional capital invested in it.

A Matter of Scale

In an environment the size of the federal government, the potential for savings is enormous simply because the scale is enormous. The Department of Defense (DOD) alone employs 2.3 million people; that's more than the population of Houston. As Tim Grance—senior computer scientist for the National Institute of Standards and Technology (NIST)—points out, the DOD is so big that the private cloud it would create would be as large as all but the biggest vendor's public cloud offerings. Kundra is targeting $20 billion worth of resources—25 percent of the federal IT budget—as being capable of moving to the cloud. The Federal Data Center Consolidation Initiative is committed to shutting down 800 data centers by 2015—almost 40 percent of the total. Of course, it's hard to comprehend all these large numbers. There's a saying about the federal government: "A billion here, a billion there, pretty soon you're talking real money."

But the challenges are also enormous. At the 2010 Gartner Data Center Conference, a survey of the data center managers in attendance showed that one of the biggest challenges in moving to a service-oriented approach is the consolidation and pooling of resources. Doesn't your company have sets of servers owned by and dedicated to a single business unit? How eager are they to give them up and instead work from a pool of servers shared by the entire company? No business has more strongly held balkanization and fiercely held fiefdoms than the bureaucracy of the federal government. Getting everyone to play together will take strong leadership from the top, time, and more than a little patience.

Kundra's strategy is that each agency must identify at least three systems to move to the cloud in the next 18 months or so. These systems need to be important core workflow systems, not just ancillary systems. Some easy wins, such as email migrations, are already being showcased. For example, www.recovery.gov simply moved its website from its existing infrastructure to the Amazon cloud. This move saved $750,000 annually—money that the government is now using to fight fraud. The Department of Agriculture moved its email from traditional systems to Microsoft's Azure cloud platform in a big way: 120,000 users moved from 21 separate email systems to one consolidated system, saving $27 million annually. Besides saving money, the cloud solution allowed USDA workers to use online versions of Microsoft SharePoint, Office Communications, and Live Meeting.

They must be dancing in the streets at the USDA. Kundra remarked that all the customers he talks to in the government "hate the enterprise software they're using. There's a huge technology gap compared to their personal lives. They feel like they're going back in time when they go into the office." That's the gap Kundra is trying to close.

The Department of Health and Human Services is using Salesforce.com to issue electronic health record requests to more than 100,000 physicians, reducing turnaround time from one year to three months. The General Services Administration is moving 17,000 users to Google Apps, saving $15 million annually. The Army Experience Center is now using a customized version of Salesforce.com to cut costs dramatically. Initial bids to upgrade the existing system, which relied on traditional infrastructure, ranged from $500,000 to over $1 million, while initial pilots of the new software-as-a-service (SaaS) solution cost as little as $54,000.

Key Areas

To start turning this governmental juggernaut in the direction of cloud computing, the report lays out several areas of focus. Here are three of the most important ones.

Security. The first area is, not surprisingly, security. Kundra spoke of "lowering the coefficient of friction" for vendors to work with the government IT organizations. Right now, vendors must be certified separately by every agency they want to sell to. This scenario greatly increases the cost and time for small companies to work with the government. The CIO used an example from the State Department, which spent $138 million over six years on paperwork certifications. These certifications were stored more securely than the systems they were supposed to protect!

It's a bit dismaying to note that, though the phrase "integrated identity management" is briefly mentioned in the official presentation, it—indeed, any mention of digital identity at all—isn't mentioned in the report. I'm sure the jungle of identity stores in the federal government has no equal anywhere, so managing identity as federal IT begins to increase its cloud presence will be critical.

Adherence to standards. An important part of such a large shift is to do it as consistently as possible, so establishing and sticking to already-established standards is another focus area. Without standards, you can't guarantee that cloud applications will be portable across service providers, and that the service providers themselves will be able to play well together. The NIST will logically be at the heart of this focus area; the world is already using its standard definitions for cloud computing, SaaS, platform as a service (PaaS), and infrastructure as a service (IaaS) delivery models, as well as the public, private, hybrid, and community cloud-deployment models. A side benefit of this federal cloud thrust is that the NIST is working with both government and private cloud computing stakeholders to create a vendor-agnostic reference architecture that can be used as a basis for many companies' cloud computing efforts.

Governance. Of course, this huge shift won't happen just by wishful thinking; it must be mandated, so governance is another focus area. A "cloud first" policy—requiring agencies to evaluate cloud computing solutions before making any new investments in traditional technology—is being put in place. This policy will be part of the budgeting process, because "the way you drive policy is through budget." As Kundra said, "Cloud is at the heart of how we're going to be provisioning IT in the coming years."

IT Priorities

It's important to gain early and substantial wins in any major project, and the federal government is no different. The strategy prioritizes categories of IT to be pushed to the cloud, based on the relative ease of the move and the benefits from such a migration.

Collaboration. The top priority is collaboration—no surprise, as the benefits of moving email, for example, to SaaS solutions are well known. Agencies are looking at moving email, customer relationship management (CRM), and office productivity tools in the near future. The next priority is workflow-related systems, such as employee verification, grants management, and claims processing. This is also the category that CRM systems fall into; the previous case studies are already using Salesforce.com successfully.

Infrastructure. The next priority is the IT infrastructure itself. Kundra spoke of "abstracting the entire infrastructure"—in other words, infrastructure as a service, from simple public websites to a much broader adoption of IaaS. This will start with application development and testing, and will eventually work toward virtualized data centers. The Department of Transportation is looking closely at this area. This kind of migration, at a much lower level of the software stack, is far more complicated than adopting cloud-based software alone; these are definitely long-term plans.

Business intelligence. BI is the next priority, where you can use the scalability of cloud solutions to attack the enormous amounts of data that federal IT is wrestling with. Kundra said the potential is huge on this front.

Information security. The lowest category in Kundra's priority list of categories to move to the cloud is information security. Identity management, mobile-computing management, and security management are all very difficult questions to answer in the context of a hybrid traditional/cloud environment. I think we're all happy to hear that this is the lowest priority—but obviously it's important that security considerations are an integral part of all these categories.

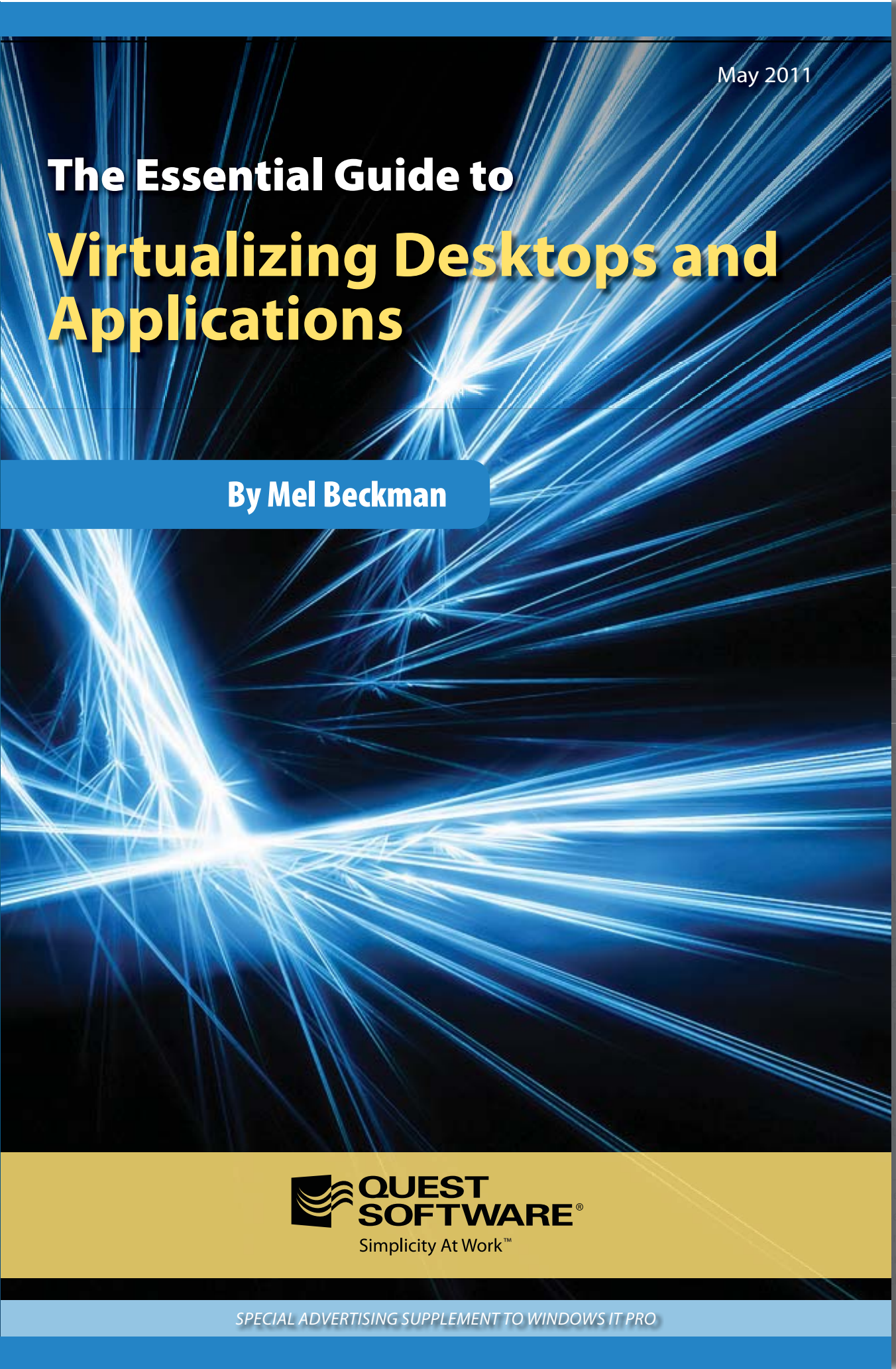
From the Top

What Kundra didn't really address in his remarks—but is brought up in the report itself—is the very difficult transition from an asset-based infrastructure to a service-based infrastructure. It's not just the technological mountain of virtualization, resource pooling, and self-service automation; it's the conversion of an extremely entrenched ownership mentality on the part of everyone in IT to an environment in which the user has a much greater degree of control over his or her own resources. In the private sector, this directly threatens the IT pro's job. It will be interesting to see what happens in the public sector, where it's not so easy to downsize a department.

It's refreshing to hear such remarks from the top brass in federal IT. I'm sure the government will find success in many areas. But it remains to be seen just how far down the stack cloud computing can penetrate in such a massive and well-entrenched computing environment. You can find the Federal Cloud Computing Strategy report and associated presentation at www.cio.gov.

InstantDoc ID 129788

SEAN DEUBY (sean@windowsitpro.com) is technical director for *Windows IT Pro* and *SQL Server Magazine* and former technical lead of Intel's core directory services team. He's been a directory services MVP since 2004.


May 2011
The Essential Guide to
Virtualizing Desktops and Applications
By Mel Beckman
QUEST SOFTWARE®
Simplicity At Work™
SPECIAL ADVERTISING SUPPLEMENT TO WINDOWS IT PRO

Traditionally, users interact directly with physical computers with many applications (such as word processing, spreadsheets, and email) running locally. The data for these applications is often also stored locally, and therefore must be managed, backed up and secured locally. Some applications may have back-end server components or may reside entirely on a server and be accessed via web browsers or locally stored application clients.

This traditional desktop operating environment, while initially convenient to set up, creates several long-term management problems:

- Automated processes for maintaining applications via centralized patch and upgrade don't scale easily; mass upgrades often consume huge quantities of network bandwidth. In addition, remote users must be treated differently than local users, resulting in delayed maintenance and roll-out.
- Data security is challenging because users can export data to devices such as writeable discs and thumb drives, leading to a proliferation of scattered, often unprotected, sensitive information.
- Data backup is difficult and unreliable, especially for the now-ubiquitous mobile users who want to access their corporate computing environment from home, hotels, airports, or any remote location.
- As desktop and mobile hardware becomes more sophisticated, the workload to maintain that hardware increases.

Even for small organizations, supporting physical desktops can become a time and resource draining task for an IT staff.

Fortunately, virtualization technologies have matured to address these problems. These technologies now enable centralized administration for convenient management, security, backup, and restoration. Fewer staff can support the same number of users, and problems can be resolved faster, reducing the total cost of ownership (TCO).

Types of Virtualization

User differences in bandwidth, application, security and performance requirements means there is no "one-size-fits-all" virtualization solution. But you can employ multiple desktop and application virtualization technologies to tailor a virtual desktop to the specific requirements of each user; this helps you avoid under- or over-delivering desktop resources. Available virtualization technologies include:

Application Streaming

For many users, the simplest and most effective path to virtualization's benefits is through application streaming. Basic applications such as word processing and email tend to work well with application streaming. You deliver the application over the network, via either streaming or some other file transfer process, and the application executes on the endpoint device—a PC, Mac, or thin client— but isolated from the device behind a thin virtualization layer. This approach can give the user desktop-quality performance in a package that looks and feels like a normal application, but functions identically no matter what device it runs on. IT staff get the benefits of centralized storage and administration: rapid deployment, enhanced security, and simplified management. Patching the application, or rolling out a new version, is invisible to the user.

Application Virtualization

Not all applications are compatible with application streaming. Some legacy software depends upon OS features (such as specific device drivers, Microsoft .NET, or SQL Server) that virtual application environments often don't support. Sometimes licensing restrictions preclude virtualization. Or an application might require local machine resources, such as network access, removable storage, or specialized hardware, not available on the endpoint device.

For these situations, application virtualization (applications running on a central terminal server session) may be a better alternative. IT can tie the presentation to a single application running in its own window, more closely simulating a local application to the end user.

Terminal Server/RD Session Host

This solution uses a shared operating system; it is good fit for users who require few applications and minimal personalization.

Hosted and Local VDI

The preceding approaches work for less sophisticated users that only require a few applications for their day-to-day computing. Advanced, so-called "power" users, generally need more. They seek a complete, self-contained virtual desktop environment that exactly mimics what they have on their local computer, with full support for audio and video media, connections to remote databases, and the ability to run arbitrary applications, from among a set of hundreds, in any combination. Hosted and local VDI delivers that capability, but effective implementations will cost more, in the form of dedicated per-user hardware, software licenses, and network capacity, than other approaches will cost. VDI can be an attractive choice if you're about to refresh your users' end-point hardware.

The key to achieving the most benefit from desktop and application virtualization at the least cost is to mix technologies to match user requirements. You should select the optimal virtualization technology for each user's working requirements, considering both local and mobile application needs. To ensure flexibility in your virtualization deployment, seek vendors who provide choices in technology, platform, storage, protocols and more. For more information on choosing vendors and determining the best types of virtualization for your environment, see the section "Evaluating Solutions" later in this document.

Balancing User and Management Needs

From a user's perspective, the ideal computing paradigm is to be able to log into *any* handy computer and immediately have access to his or her personal computing or application environment in exactly the state last used. Users don't want to deal with maintaining multiple environments and keeping documents and settings synchronized between them.

Management, on the other hand, needs to protect critical data from loss or inadvertent disclosure to the wrong people, both to meet internal business requirements and also to comply with external regulations such as Sarbanes-Oxley, HIPAA, and PCI/DSS. Comprehensive auditing and reporting is also required to demonstrate compliance and provide peace of mind about security.

Striking a Balance with Virtualization

There's no denying that user and management objectives often compete with—or even contradict—each other. Fortunately, the variety of available technology choices can enable you to balance the needs of users and IT management. The most common advantages of virtualization technologies are:

- **Consistent user desktop interfaces—** Desktop interfaces are no longer dependent on user hardware and operating system components, and therefore they are more consistent. Virtualization pushes resources off of local computing devices and into the virtualization infrastructure.
- **Secure, central storage of data—** All user data is stored centrally, where it can be easily backed up and secured using robust encryption technologies. It is always easier to secure a centralized server than thousands (or even tens of thousands) of traditional desktop machines.
- **Control and security of the desktop—**IT can reduce the risk of malware by restricting users from installing unauthorized software.
- **Centralized management of applications—**Applications are maintained centrally and therefore are easier to deploy, test, update, patch and manage. This one-to-many model (as opposed to the many-to-many model of physical desktops) ensures that all of your users' applications are the same version and enables you to rapidly roll out modifications or new use policies, You no longer have to push updates and hope your users will accept them.
- **Reduced hardware costs—** Because hosted virtual desktops do not require processing power, hardware refresh cycles are much less frequent; one cycle can last as long as 5 to 10 years. Refreshes are dramatically less expensive as well, because "thin clients" are roughly one-third to one-half the cost of traditional physical PCs.
- **Overcoming network issues—** Because all virtualization technologies are network-centric (including

local VDI options when connected), they are susceptible to attacks by hackers and latency issues. Vendors now offer network gateways, optional multi-factor authentication and highly secure protocols with encrypted data to help secure the environment. They also try to improve network latency, with varying degrees of success. Ensuring a positive user experience regardless of bandwidth constraints will improve user adoption and acceptance.

- **Economies of scale—** One overall benefit of desktop and application virtualization is economies of scale and operational efficiencies, similar to those gained with server and storage virtualization. With all of your user data in one place, you can purchase storage en masse for less than the cost of distributing disk drives to user machines. Maintenance support becomes much less expensive as well: no more trudging out to individual desktops, or tracking down traveling laptop users, to patch, repair, update or back up their systems. When a user device fails, you can simply issue a new unit and have the user log in. These savings can offset the cost of delivering a variety of virtualization solutions.

Why a Deployment Fails (and Ensuring It Doesn't)

Until recently, desktop and application virtualization has had mixed reviews for users and IT administrators alike. Some of the most common reasons for failed deployments have been:

Misunderstanding User Requirements

Many virtualization projects fail not because the virtualization technology breaks, but because the project plan doesn't properly consider the distribution of CPU, memory and storage as based on user needs. If you deliver virtualization as a *fait accomplis*, without understanding your users' wants and needs, you may well discover that the virtualized environment prevents users from doing one or more aspects of their jobs. Once you've alienated users, it's very difficult to regain their cooperation.

To avoid this pitfall and ensure a successful deployment, you must involve users in the virtualization planning process at the earliest opportunity and gain their buy-in. The planning process should include a formal assessment of existing applications and usage models. Understanding your users' needs and wants will help you determine the correct technology or technologies to deploy.

Lack of Necessary Tools

A second common reason virtualization projects fail is underestimating the scope and complexity of administration processes. Although virtualization ultimately simplifies administration, the processes are quite different from those in traditional desktop support. Budget enough time and money for good management tool sets, as well as a consistent and easy-to-understand set of interfaces that minimizes staff retraining and provides automation capabilities. Don't eliminate your TCO reductions with inadequate management tools.

Rushing the Process

The last and most common cause of virtualization project disaster is attempting a one-time massive conversion. No planning process can be perfect, and you'll undoubtedly miss some user requirements. Deploying gradually in a phased approach lets you gain procedural experience as you go.

You should also take the time to minimize end user rejection. Don't force users to "go to" the virtualization solution. Instead, put it at their fingertips by integrating it into their existing workflow; this maintains a seamless working environment that doesn't force users to shift mental models.

Evaluating Solutions

The number and breadth of virtualization products is truly astounding. Some offerings are specialized stand-alone solutions aimed at a single use case. Others have broader scope, but are tied to particular virtualization architectures, such as VMware's ESX/vSphere. Still others are oriented around a particular end-user hardware platform or thin client.

When evaluating virtualization solutions, some of the attributes you should consider include:

- A breadth of technology choices to meet the largest number of your specific user requirements. Vendors may support hosted and local VDI, Terminal Server/RD Session Host, application virtualization and streaming, blade PCs, and more.
- Per-user preference profiles so that a user's unique operational choices and allowances follow them

- Multi-factor authentication to ensure device and data integrity in hostile environments
- Automation capabilities for scripting repetitive administration tasks, including user provisioning, policy changes, and asset control
- A minimal number of products and consoles needed to operate the environment. Having multiple consoles can complicate management, add training expense, and quickly erode any savings
- Reporting and auditing tools to track user access and security events, demonstrate compliance with regulations, and monitor performance and availability
- LAN/WAN optimization via compression, deduplication, caching and other techniques to reduce the effects of network latency and maximize performance

Conclusion

Reaping the maximum benefits from desktop and application virtualization requires carefully matching a virtualization approach to the user requirements. No one approach fits all user needs or management budgets, so you must balance performance, capabilities, and costs to fit your situation. At the same time, desktop and application virtualization is a complicated marketplace, with many vendors, and a steady stream of innovations that require constant evaluation. This is where comprehensive management tool sets can help, by integrating virtualization technologies into a centralized administrative tool set.

How will you pay for all this? It's true that both desktop and application virtualization require a significant up-front investment in time and money. But when you consider the TCO savings that accrue from virtualization payback—faster deployment, reduced support loads, and better economies of scale—you may well find that virtualization pays for itself in the long run.

About the Author

Mel Beckman is a senior technical director for Penton Media.

READER TO READER

Byte Conversions Made Easy

Microsoft and other application vendors represent disk space and memory sizes in bytes, kilobytes, megabytes, gigabytes, and so forth. For example, 1,024 kilobytes equals 1MB. It's a common task to convert these values to different units. For example, you might have to convert 16GB into kilobytes.

Bill Stewart

Storage vendors add an interesting wrinkle to the conversions because they calculate these units differently. They typically use factors of 10 instead of 2. For example, a "kilo" represents 1,000 bytes instead of 1,024 bytes. This difference can cause problems when you need to know, for example, how much tape is needed to back up a database. A database that uses 400GB on a disk won't fit on a 400GB tape because 400GB means 409,600 megabytes to the OS but only 400,000 megabytes to a storage vendor.

I often use a calculator to convert between bytes, kilobytes, and so forth. To eliminate calculator errors and save myself some time, I decided to write an HTML Application (HTA), ByteCalc.hta, to perform these conversions. ByteCalc.hta converts values using both factors of 2 (kilo = 1,024 bytes) and 10 (kilo = 1,000 bytes).

To run ByteCalc.hta, simply double-click it from Windows Explorer or enter its filename at a command prompt. (You can download the HTA by going to www.windowsitpro.com, entering 129737 in the InstantDoc ID box, clicking Go, then clicking the *Download the Code Here* button.) In the HTA's UI, which Figure 1 shows, enter a number in the Value field, choose the unit in which the number is expressed (e.g., gigabytes, megabytes), and click the Calculate button.

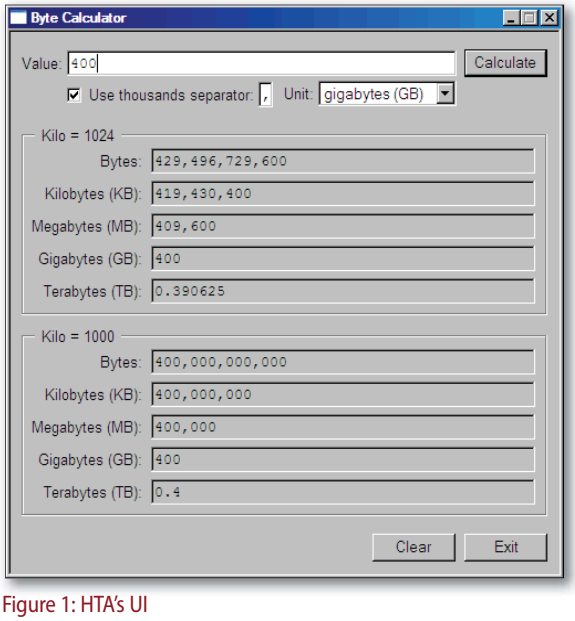


Figure 1: HTA's UI

ByteCalc.hta uses the <input> and <select> HTML elements combined with JScript (Microsoft's version of JavaScript) code to perform the conversions. To calculate the proper values, it uses the <select> element's currently selected <option> element to determine which values get placed into the corresponding fields on the form. Table 1 shows the formulas that ByteCalc.hta uses to convert bytes. Table 2 shows the formulas it uses to convert megabytes. As you can see in Tables 1 and 2, ByteCalc.hta either divides or multiplies by a factor (depending on whether kilo = 1,024 or 1,000) to achieve its results.

Table 1: Converting from Bytes

Number (*n*)	Kilo = 1,024	Kilo = 1,000
Bytes	None	None
Kilobytes	$n / 2^{10}$	$n / 10^{3}$
Megabytes	$n / 2^{20}$	$n / 10^{6}$
Gigabytes	$n / 2^{30}$	$n / 10^{9}$
Terabytes	$n / 2^{40}$	$n / 10^{12}$

Table 2: Converting from Megabytes

Number (*n*)	Kilo = 1,024	Kilo = 1,000
Bytes	$n * 2^{20}$	$n * 10^{6}$
Kilobytes	$n * 2^{10}$	$n * 10^{3}$
Megabytes	None	None
Gigabytes	$n / 2^{10}$	$n / 10^{3}$
Terabytes	$n / 2^{20}$	$n / 10^{6}$

Listing 1: Code to Customize in ByteCalc.hta

```
var THOUSANDS_SEPARATOR_DEFAULT = true,
  THOUSANDS_SEPARATOR = ",";
```

By default, ByteCalc.hta uses a comma (,) as the thousands separator and includes thousands separators in its results. If you don't want to use thousands separators, clear the *Use thousands separator* check box before clicking the Calculate button. If the *Use thousands separator* check box is selected, you can enter a different character for the thousands separator.

You can easily configure ByteCalc.hta not to use thousands separators by default. Open ByteCalc.hta in Notepad (or another plain-text editor) and locate the two lines of code shown in Listing 1. Change the THOUSANDS_SEPARATOR_DEFAULT variable from *true* to *false* (the words *true* and *false* must be lowercase). If you want to use a thousands separator but you want it to be some other character by default, replace the comma between the

Tell the IT community about the free tools you use, your solutions to problems, or the discoveries you've made. Email your contributions to r2r@windowsitpro.com.
If we print your submission, you'll get $100.

Submissions and listings are available online at www.windowsitpro.com. Enter the InstantDoc ID in the InstantDoc ID search box.

double quotes to the character you want to use.

—Bill Stewart, IT infrastructure group, Emcore

InstantDoc ID 129737

Automatic Elevation of a .cmd Script

Pieter Demeulemeester

Microsoft introduced User Account Control (UAC) in Windows Server 2008 and Windows Vista to prevent unauthorized computer changes. As a result, application developers need to include a manifest that identifies the privilege level that an application needs to run under. When that application runs, UAC displays a dialog box either asking for consent to continue (if the user has the necessary privileges) or for elevated credentials (if the user doesn't have the necessary privileges).

A manifest is an XML-formatted file that accompanies an application. Figure 2 shows the manifest for cmd.exe. Notice that the value for the *requestedExecutionLevel* element is *asInvoker*. This means that the application doesn't need to run under elevated permissions. It runs under the credentials of the user who started the program. This brings about a problem: Because Windows doesn't elevate cmd.exe, a .cmd or .bat script won't run in elevated mode if you double-click it. Instead, you have to right-click the script, select the *Run as administrator* option from the context menu, then confirm that you want to run it.

To make it easier to run .cmd scripts in elevated mode, I wrote code that uses Windows' WhoAmI utility to detect whether a script is running in elevated mode and, if not, forces elevation with Johannes Passing's free elevate .exe tool. Listing 2 contains this code in a sample script (Test.cmd) that you can run and use as a template.

Here's how Test.cmd works. The line in callout A uses the *WhoAmI /Groups* command to retrieve the user groups to which the current user belongs. (It gets this information from the access token.) The presence of the group *Mandatory Label\High Mandatory Level (SID S-1-16-12288)* means that the user started the script in elevated mode (i.e., started it with the *Run as administrator* option). So, the line in callout A searches the *WhoAmI /Groups* command's output for the string "S-1-16-12288". It sets the ERRORLEVEL environment variable to 0 if it finds the string; otherwise, it sets the variable to 1.

The If command in callout B handles that environment variable. If the ERRORLEVEL variable's value is 0 (i.e., in elevated mode), the script jumps to the :ELEVATED label and runs the code underneath it. In this case, the IPConfig utility is executed, as callout C shows.

If the ERRORLEVEL variable's value is 1 (not in elevated mode), the *elevate.exe %0 %CD%* command executes. The %0 variable resolves to the script's pathname (e.g., C:\SCRIPTS\Test.cmd) and elevate.exe runs the script again but this time in elevated mode. (I'll explain the %CD% variable shortly.) In this second run, the ERRORLEVEL environment variable will be 0, so the code under the :ELEVATED label will run.

Listing 2: Test.cmd

```
@Echo Off
A WhoAmI /Groups | Find "S-1-16-12288" > nul
B If "%ERRORLEVEL%"=="0" (Goto :ELEVATED)
    Else (elevate.exe %0 %CD%)
Goto :END

:ELEVATED
    Pushd %1
C   ipconfig.exe /registerdns
    Pause
Goto :END

:END
```

Rerunning a script with elevate.exe has one disadvantage: The command prompt automatically changes to the C:\WINDOWS\System32 folder, which can cause a problem if a script needs files from the folder in which it's located. To prevent any problems, I use the %CD% environment variable in the elevate.exe command and *Pushd %1* in the code under the :ELEVATED label. The %CD% variable is populated with the path of the folder that the command prompt currently points to. Thus, when you run a script by double-clicking it, %CD% is populated with the path of the folder in which the script resides. The script can access that path using the %1 environment variable. So, the *Pushd %1* command sets the command prompt back to the initial folder (in this example, C:\SCRIPTS).

To use Test.cmd as a template, follow these steps:

1. Download Test.cmd by going to www.windowsitpro.com, entering 129738 in the InstantDoc ID box, clicking Go, then clicking the *Download the Code Here* button.
2. Download elevate.exe from jpassing.com/2007/12/08/launch-elevated-processes-from-the-command-line, and place it in the folder that contains your template.
3. Replace the IPConfig command in callout C with the code you want to run in elevated mode.

If you just want to test the code, you can omit step 3.

With this template, your scripts will always run elevated. You'll no longer need to elevate them by right-clicking and selecting *Run as administrator*.

—Pieter Demeulemeester, systems engineer, Brothers of Charity

InstantDoc ID 129738

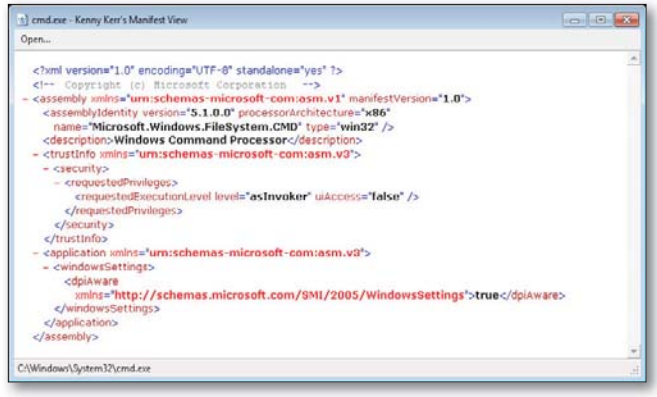


Figure 2: Manifest for cmd.exe

- RAID
- Outlook
- XenApp
- Software Installation

ANSWERS TO YOUR QUESTIONS

Q: How can I let non-administrators install software on their machines?

A: Changes in the way Windows Vista and Windows 7 were designed compared with earlier versions have led many organizations to stop letting their users be local administrators. It just isn't necessary for your users to be administrators, and having all your users as local administrators of their machines increases the risk of malware and system instability.

One frequent request is to allow non-administrators to install software on their machines. However, installing software is one of the key reasons computers become unstable and subjected to malware.

The best way to let users install corporate software is to use Group Policy, System Center Configuration Manager (SCCM), or Microsoft Application Virtualization (App-V), which can deploy software as a trusted install. Another option is to use UAC for an administrator to provide over-the-shoulder elevation to install the software.

You can configure the system to always install with elevated permissions using the HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Installer\AlwaysInstallElevated registry value (it can also be set under HKEY_CURRENT_USER), but this isn't recommended because you incur extra risks if application installs run as System, with the access to system areas that permission brings. For more detail on this setting, see "How to Manage Windows Installer Local Policies" (support.microsoft.com/kb/227181).

—John Savill

InstantDoc ID 129601

Q: How do you show multiple time zones in Calendar view in Microsoft Outlook 2010?

A: When you work with multiple locations across different time zones, sometimes it's helpful to display those time zones concurrently in your calendar. Outlook lets you show a side-by-side hourly scale beside the calendar for easy reference. Having Outlook show two time zones at once can be simpler than having to work out the difference or look it up each time you're considering the equivalent time at the second location. Those of you in Canada are probably familiar with the media saying, when referencing a national program schedule, "one half-hour later in Newfoundland." I'll use Newfoundland as my secondary time zone for this tip.

Outlook 2010 lets you add a second time zone to the calendar view and provide a label for the time zones displayed. The options to add and label time zones are found in File, Options, Calendar. Scroll through the Calendar Settings options until you reach the heading Time Zones.

Outlook by default assumes that the time zone of your workstation is the main time zone and doesn't assign a label to it. Below this time zone setting is a check box with the option to *Show a second time zone to the view*. You can also assign an optional label. Figure 1 shows the two time zones side by side along the left side of the calendar view, labeled as Home and Newfies for the time zone of Newfoundland.

The label, if you choose to add one, appears at the top of the column forming the Y-axis in the calendar grid. I can easily see that the time at our (imaginary) office in Come-By-Chance, Newfoundland, is 1:30pm. while we have our 9:00am meeting at the home office location on Wednesday. The settings for the secondary time zone feature can be found in the registry at the following location: HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Outlook\Options\TimeZone\.

If you need users to have this setting preconfigured, you can do so using a .reg file through logon scripts or Group Policy.

—William Lefkovics

InstantDoc ID 129615

Q: How can I check the version of my System Center Configuration Manager (SCCM) 2007 installation?

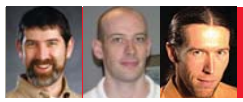
A: There are now several different versions of SCCM 2007—RTM, SP1, SP2, R2, and R3. If you launch the SCCM administration console and select Help, About System Center Configuration Manager, you can check the version. The versions and their numbers are:

- RTM - 4.00.5931.0000
- SP1 - 4.00.6221.1000
- SP2 - 4.00.6487.2000

To check if you're using R2 or R3, open the properties of the SCCM site. The General tab once again shows the version, but also shows if R2 or R3 are installed.

—John Savill

InstantDoc ID 129673



William Lefkovics | william@mojavemediagroup.com
John Savill | jsavill@windowsitpro.com
Greg Shields | virtualgreg@concentratedtech.com

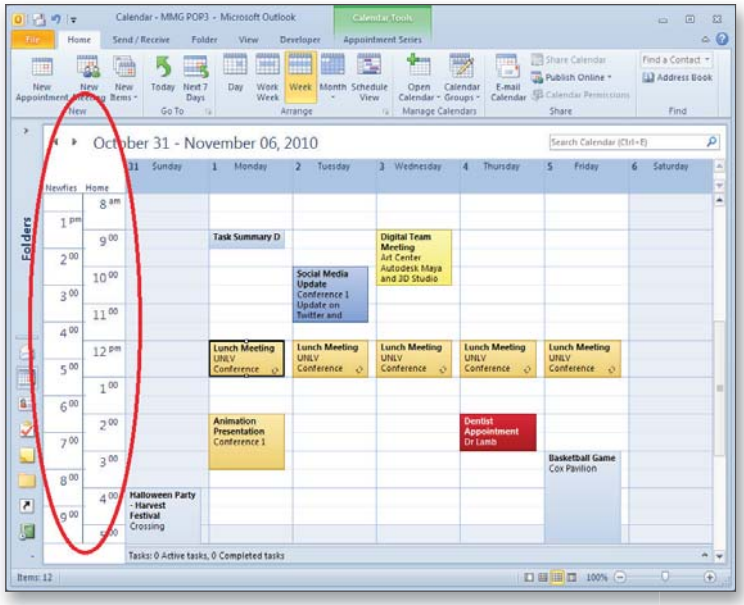


Figure 1: The Calendar view with two time zones displayed

Q: What command-line utilities are available in Citrix XenApp 6?

A: If managing your Citrix XenApp 6 server from the Citrix Delivery Services Console isn't your thing, you should know that many of the commands you've used in XenApp's previous versions remain available in this new release.

Specifics about each command are available at the Citrix website (support.citrix.com/proddocs/index.jsp?topic=/xenapp6-w2k8-admin/ps-commands-wrapper-v2.html). The following list of command-line utilities is available on a Citrix XenApp 6 server for administration:

- altaddr: Specify server alternate IP address.
- app: Run application execution shell.
- auditlog: Generate server logon/logoff reports.
- change: Change client device mapping.
- ctxkeytool: Generate farm key for IMA encryption.
- ctxxmlss: Change the Citrix XML Service port number.
- dscheck: Validate the integrity of the server farm data store.
- dsmaint: Maintain the server farm's data store.
- enablelb: Enable load balancing for servers that fail health-monitoring tests.
- icaport: Configure TCP/IP port number used by the ICA protocol on the server.
- imaport: Change IMA ports.
- query: View information about server farms, processes, ICA sessions, and users. The query command uses a set of extra nouns to identify which XenApp component should be queried for data. Those nouns are: query farm, query process, query session, query termserver, and query user.

These command-line utilities are available on each server, but this version of Citrix XenApp leans heavily on Windows Power Shell for many command-line functions. PowerShell exposure for Citrix XenApp is found in the XenApp 6 PowerShell SDK, which can be downloaded from Citrix (community.citrix.com/display/xa/XenApp+6+PowerShell+SDK).

—Greg Shields

InstantDoc ID 129497

Q: Which PerfMon counters does XenApp 6 add to a Windows server?

A: Installing Citrix XenApp 6 to a Windows server also adds six new categories of PerfMon counters. These new categories measure metrics that relate to the processing of XenApp functions. The six categories are:

- Citrix CPU Utilization Mgmt User
- Citrix IMA Networking
- Citrix Licensing
- Citrix MetaFrame Presentation Server
- ICA Session
- Secure Ticket Authority (for servers running the Secure Ticket Authority)

Each category includes a set of individual counters that can be turned on for the server. You can get detailed information about each counter on the Citrix site.

—Greg Shields

InstantDoc ID 129496

Q: I've lost a disk in my Windows Server 2008 software RAID 5. How do I repair it?

A: If you're using software RAID 5, you have three or more dynamic disks configured as a single fault-tolerant volume that data and parity information is stored on. If you lose a single disk from the set, no data is lost thanks to the data and parity information on the remaining disks, which can be used to calculate the data on the lost disk. If you need to replace a disk (like I just did after one of my Western Digital Black drives died after six months), follow the procedure below:

1. Replace the dead disk with a new one in the server.
2. Access the Disk Management node of Server Manager.
3. Your replacement disk will be found, and you'll be prompted to initialize the disk.
4. Once it's initialized, right-click the disk and select Convert to Dynamic Disk.
5. Ensure that only your new disk is selected to convert, and click OK.
6. Scroll down to the disk that's missing for your RAID 5 set, right-click it, and select Repair Volume.
7. Your new disk will be listed to be used as the replacement. Make sure it's selected, and click OK.
8. Your RAID 5 volume will go into a Resyncing state, which can take a while—it has to repopulate the data/parity information on the new disk to make the RAID 5 volume fault tolerant again. Right-click the missing disk, which no longer has any associated volume, and select Remove Disk.

Try and minimize the workload on the RAID 5 while it's resyncing because a heavy load will slow down the rebuild.

—John Savill

InstantDoc ID 129690

Q: How can I configure Windows 7 or Windows Vista to automatically wake at a certain time and run a task?

A: Windows Vista and later support wake timers that scheduled tasks can use, allowing a system to automatically wake from sleep or hibernation at a certain time. This can be useful to wake machines so they can check for updates or changes in policy.

To use a local scheduled task:

1. Launch Task Scheduler (Start, Accessories, System Tools, Task Scheduler).
2. Select the Create Task action.
3. Name the task under the General tab and, optionally, provide a description.
4. Select the Triggers tab, select New, and specify to begin the task on a schedule. Select Daily or Weekly (or whatever you need) and the recurrence. Specify the start time (e.g., 2:00:00am) and click OK.
5. Under Actions, select the program or task you want to run. For example, to install important updates from Microsoft, I could set the program to

```
%windir%\system32\wuauclt.exe
  /detectnow
```

You could always have a script that runs the install, then runs

```
shutdown -s
```

to shut down the machine. Feel free to use other options that work best for your environment.

6. Click the Conditions tab, select *Wake the computer to run this task*, and click OK.

—John Savill

InstantDoc ID 129670

Q: Can I share my Tasks with other users in Microsoft Outlook 2010?

A: Along with the Journal feature, Tasks are one of the most underutilized features within Outlook. Some users depend on them wholly, and others completely ignore the option. The addition of the To-Do List in Outlook brings the Task list into the main interface, so it no longer has to be out of sight, out of mind. The To-Do List can be viewed in the To-Do Bar, which you can customize; to see how to do so, check out "How do I configure views in Microsoft Office Outlook 2007's To-Do Bar using either menu commands or the registry?" (InstantDoc ID 98436). Making tasks even more useful, they can be shared or assigned to others in Outlook.

If you're using a Microsoft Exchange Server account, you can share your Tasks with other users, just as you can share any folder in Outlook. Right-click the Tasks folder in the folder list and select Properties at the bottom of the context menu to open the Tasks Properties dialog box. Select the Permissions tab to share this folder; the Permissions tab is present only if Outlook is using an Exchange Server account. For example, a user named Tinker Juarez can now select Open, Other User's Folder, which reveals a small window, and select the folder shared to him.

In this example, Tinker Juarez can open the Tasks folder shared to him and manipulate the content based on the level of access that has been shared to him. In the Tasks view for Tinker Juarez's Outlook 2010 client, he'll see a Shared Tasks section in the Navigation Pane below the My Tasks section.

The preset options for permission levels for sharing a folder in Outlook 2010 are fairly comprehensive. They provide for almost all combinations of attributes that you can assign to an Outlook object. The list is as follows:

- Owner—You can create, read, modify, and delete all items and files, and create subfolders. You can also change the permission levels others have for the folder.
- Publishing Editor—You can create, read, modify, and delete all items and files, and create subfolders.
- Editor—You can create, read, modify, and delete all items and files.
- Publishing Author—You can create and read items and files, create subfolders, and modify and delete items and files that you created.
- Author—You can create and read items and files, and modify and delete items and files that you created.
- Contributor—You can only create items and files. You won't see the contents of the folder.
- Reviewer—You can only read items and files.
- Custom—You can perform activities that are defined by the folder owner. The create, read, modify, and delete attributes can be assigned in any combination.
- None—You have no permissions and you cannot open the folder.

This simple method of sharing folders is standard across all types of Outlook items. But what if you don't want all items in a folder shared?

Some tasks might be personal or confidential in nature, and you might want to hide the contents of such tasks from people who otherwise have access to the Tasks folder. Individual tasks can be assigned a Private status, which makes them available only to the task owner. In Outlook 2010, you set this property within the Task form itself. You set a task to Private by clicking the Private option in the Tags section of the Tasks tab of the Office ribbon.

This option still exists when using Personal Folders; however, there's no option to share tasks with others using a PST. Interestingly, the Private setting is maintained when a PST is imported into a mailbox, however. When Tinker Juarez opens the Tasks folder shared to him by another user, any tasks marked as Private won't be visible in his view.

Alternatively, you can create an additional folder for tasks that are intended as private. This folder can be a subfolder of the original Tasks folder or can be placed elsewhere. To create a new Tasks folder (or any Outlook folder type), right-click in the navigation pane under the account you want to add the folder to and select the New Folder option. This opens the Create New Folder dialog box.

Provide a name for the folder, and then select the item type as Task Items to ensure that Outlook uses a Task window—called an IPM.Tasks form by developers—for content saved to this folder and for requests for a new item from this folder. If your primary Tasks folder is shared out, you can save private tasks to a separate folder without having to worry about the necessity of assigning the Private tag to each task.

—William Lefkovics

InstantDoc ID 129613

Windows Intune

Brings PC Management Into the Cloud

A more complete solution for more customers

by Paul Thurrott

The fact that Microsoft is in the midst of a dramatic retooling of its product offerings should come as no surprise: The company is moving rapidly to establish itself as a dominant provider of cloud services in addition to its more traditionally delivered client and server solutions. Today, the company offers both hosted services—cloud-based versions of its most popular server products, such as Exchange Server and SharePoint Server—and entirely new cloud-hosted platforms, such as Windows Azure and SQL Azure, among other offerings.

Microsoft has long championed a unique opportunity for customers that its competitors simply can't match. In addition to the sheer volume of its disparate offerings, Microsoft also offers customers a range of choices that span both traditional, on-premises offerings and hosted cloud services, as well as a hybrid deployment model in which both on-premises and hosted offerings can be mixed and matched within a corporate environment. Companies such as Amazon and Google, whose product offerings exist almost solely in the cloud, simply have no answer to this need.

As Microsoft's cloud-based offerings have matured and expanded, the company has begun moving into some interesting new product areas. This year, it will replace its Business Productivity Online Standard Suite (BPOS) and other related products with a more cohesive (and more easily licensed) Office 365 service, pushing its dominant Office family of products firmly into the cloud as well. And with Windows Intune, Microsoft has begun the enormous task of bringing its mature PC management capabilities, available today in its on-premises System Center offerings, to the cloud as well.

Over time, Microsoft seeks to bring all the functionality of the System Center servers to the cloud, minus the complexity where possible. And that's perhaps the most intriguing general idea behind Intune: This isn't just a hosted port of Microsoft System Center Configuration Manager (SCCM); in fact, in its current state, it's nowhere near as powerful. Instead, it's a brand-new product, optimized for specific scenarios, and delivered along with a clear plan for the future.

Indeed, the level of transparency we're seeing from the Windows Intune team is notable and in sharp contrast to the veil of silence that comes out of other Microsoft product groups, including those for Windows Phone and Windows Client. Microsoft understands that this is a quickly evolving market, and the company intends to deliver a number of interesting new features over the next few years, closing the gap with System Center and making Intune, over time, a more complete solution for more customers.

We'll get to that in a bit. But first, let's discuss what Windows Intune brings to the table today, and what size businesses will benefit most from its initial feature set.

Figure 1: Windows Intune administration console

What Is Windows Intune?

Windows Intune is a cloud-based PC management solution that Microsoft targets at businesses of all sizes. It consists of a simple web-based management console interface, a client installation (or agent), and a bundled client security solution based on Microsoft Forefront and a Windows 7 Enterprise upgrade subscription for each managed PC. For a small additional per-PC cost, you can also add a Microsoft Desktop Optimization Pack (MDOP) subscription, which provides access to a rich set of somewhat related PC management, virtualization, and troubleshooting tools.

Unlike Microsoft's on-premises System Center offerings, Windows Intune isn't based on, nor does it require, Active Directory (AD). In fact, it doesn't require (or support) any on-premises server infrastructure at all. Instead, as a cloud-based service, Intune exists entirely on Microsoft's data centers, and your only access comes via the web.

There are, of course, some integration bits that will aid deployment and, over time, PC management as well. You can deploy the Windows Intune agent to the PCs in your environment using an existing electronic software distribution (ESD) system, including those made by Microsoft or any third party. And although Intune doesn't integrate with AD per se, it is at least AD-aware. That is, the Intune policies that I discuss later will always respect any existing AD Group Policies, in that Group Policies take precedence over all Intune policies.

In its first-version guise, Intune offers a number of key features, including the ability to manage PCs regardless of their physical location or connectivity to the corporate network, centralized health monitoring of connected PCs, the ability to manage which updates are (and aren't) installed on connected PCs in a granular fashion, a bundled Endpoint Protection client that's based on Forefront technology, highly configurable alerts with remote assistance mediation capabilities, client software inventorying, client software license management, simple client policy management, and excellent reporting functionality. In the next few sections, I step through each of these capabilities and discuss how the simple web-based management interface works.

Using Windows Intune

After you sign up for Intune, you can access the Windows Intune management experience by browsing to manage.microsoft.com in your favorite web browser and logging on. Representatives of a single company will be presented with the Intune administration console, which Figure 1 shows. Microsoft also has a separate Intune multi-account console, which Figure 2 shows, aimed at partners who will be managing multiple environments for customers. This multi-account console lets you sort the available environments by various criteria, including name (the default) and health; environments with problems will appear at the top.

Whether you're a single-company rep or a multi-account partner, you'll eventually need to manage a single environment—which is where the Windows Intune administration console comes into play. This console is about as simple as such interfaces get, with a navigational panel that's divided into what Microsoft calls *workspaces,* a main information panel, and a context-sensitive tasks panel. If you've used any Microsoft console, this will be familiar territory. However, Intune also targets small companies without an IT infrastructure, so the console is friendly enough that virtually any semi-technical user should be able to get started quickly.

System overview. Intune's workspaces map closely to the product's capabilities. The System Overview workspace provides a quick overall look at the health of the environment, giving you a single place to examine the security status, agent health, and pending updates for each connected PC, as well as any alerts. You can also quickly create computer groups—used to segregate connected PCs into logical groupings for policy purposes—or view a report from this workspace.

PC management. You can view and manage computers from the Computers workspace. You can also create computer groups, copy individual computers or a range of PCs into a group (only one group; this isn't a hierarchical system but is

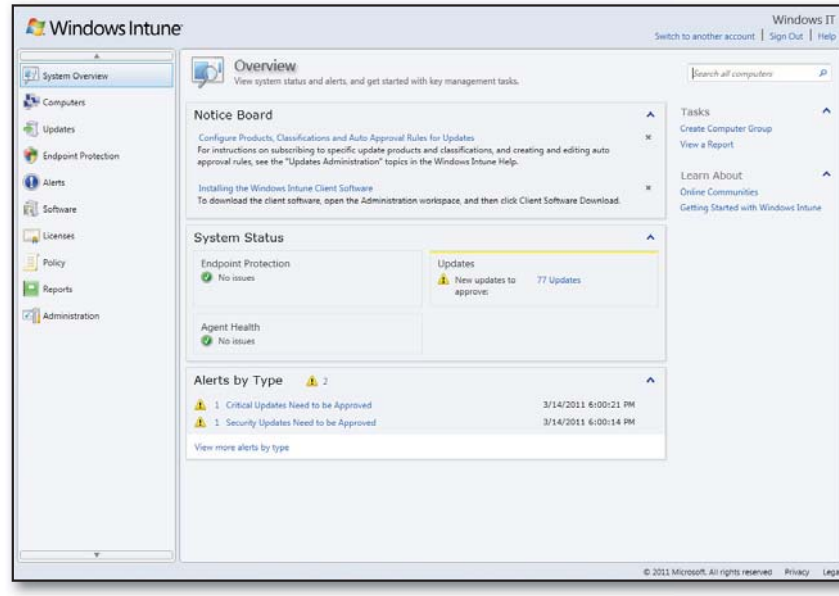


Figure 2: Windows Intune multi-account console

instead flat), and view other issues related to managed PCs. The primary activity here is PC group management. By default, each PC that downloads and installs the Intune agent is assigned to the Unassigned Computers group; although you can (and often should) assign policies to PCs in this group, even the simplest of environments would benefit from a more granular grouping. In my demonstration environment, I created groups based on geographic location—Boston, San Francisco, and so on—but grouping can be custom tailored to the needs of your environment.

Looking at the PCs within a group, a rich selection of information is available, including each PC's OS, machine name, group membership, and alert, update, and security status. For machines that need help (e.g., updates that need approval), you can click a link to view the issue(s) and mediate accordingly. For example, you can select multiple new or pending updates and click an Approve toolbar button to apply the change.

You can also view more detailed information about each PC, including malware, alerts, a full hardware profile, and a complete software inventory. Each of these items can also be used as a pivot of sorts. So if, for example, you discover a certain version of Adobe Reader, you can click it in the list to see exactly which other PCs in your environment also have that software version installed.

Software updates. In keeping with its core mission, Windows Intune can be used to view pending service packs, hotfixes, and other updates for your connected PCs, as well as perform related tasks. The Updates workspace provides you with a running total of how many new updates are waiting to be installed in your full environment, giving you the opportunity to approve (or decline) them in bulk or step through them one at a time to verify the need.

The Updates workspace also provides granular controls for determining the types of products for which you'd like to manage updates. You can be Draconian (all categories) or more measured, select updates by classification (service packs, tools, and so on), and create rules for automatically approving certain types of updates (based on the provided categories and classifications).

Client security protection. You also gain, as part of your Intune subscription, the right to optionally install a special version of the Forefront Endpoint Protection (FEP) client, called Windows Intune Endpoint Protection, on each connected PC. There are a variety of ways in which you can determine whether to install this client, however, including the ability to install only when an acceptable security client isn't found. Alternatively, you can simply choose to disable whatever solution is on the PC(s) and replace it with Endpoint Protection.

In the Endpoint Protection workspace, Intune lets you quickly view and act on any security-related issues. In my testing period, I didn't come across anything notable here, but I discovered that malware and dubious PCs are called out separately when needed. Intune maintains a list of the most recent malware instances, including whether or not they've been resolved.

Windows Intune's administration console is as simple as such interfaces get; if you've used any Microsoft console, it will be familiar territory.

Alerts and remote assistance. Windows Intune is configured to trigger alerts in response to specific events that compromise the overall health of your environment or in response to user requests for remote assistance. In the main Alerts workspace view, unresolved alerts are listed according to severity, with warnings at the top and informational alerts at the bottom. Alerts are also divided into two types: those that actively require a response and those that don't.

Out of the box, Intune is configured with almost 400 different alerts, most of which are disabled by default, and a set of basic notification rules. You can configure who is notified of alerts (recipients), why (the rules), and how (only via email, currently). A basic notification rule, such as All Critical Alerts, will trigger whenever a critical alert occurs and will fire off to whichever users (i.e., email addresses) you configured. You can't currently edit the default rules, other than to specify who gets the email.

The Alerts workspace also provides a few related bits of functionality. You can specify a list of Intune administrators (unrelated to actual administrators in your environment) by providing an email address for each one. (Note that the email address for each Intune administrator should also be associated with a Windows Live ID.) Granting this access allows a user to log on to the Intune management site (assuming the email address is also a Windows Live ID) and manage computers. It also places that user in the list of potential alert recipients.

The Alerts workspace provides a manual link for downloading the Windows Intune client agent and its associated certificate. It runs on any 32-bit or 64-bit version of Windows 7 (Professional, Enterprise, or Ultimate), Windows Vista (Business, Enterprise, or Ultimate), or Windows XP Professional (SP2 or SP3).

Finally, Alerts provides an interface through which administrators can respond to user requests for remote assistance. Users trigger these requests via the Windows Intune Center software that's installed along with the agent; for administrators, the alert will appear in both the System Overview and Alerts workspaces in the administration console. (The Intune Center, which Figure 3 shows, also includes front ends for both Windows Update and the Windows Intune Endpoint Protection client.)

Software inventory. Intune's software inventory functionality leverages technology from MDOP's Asset Inventory Service (AIS), providing you with an interesting view of the software inventory in your environment. You can sort via installation count (to find out which software is most popular on your connected PCs) or by name, publisher, or category. You can also deep-dive into a particular application and find out exactly which computers it's installed on, along with its version and whether it's installed as part of a virtual Microsoft Application Virtualization (App-V) application package.

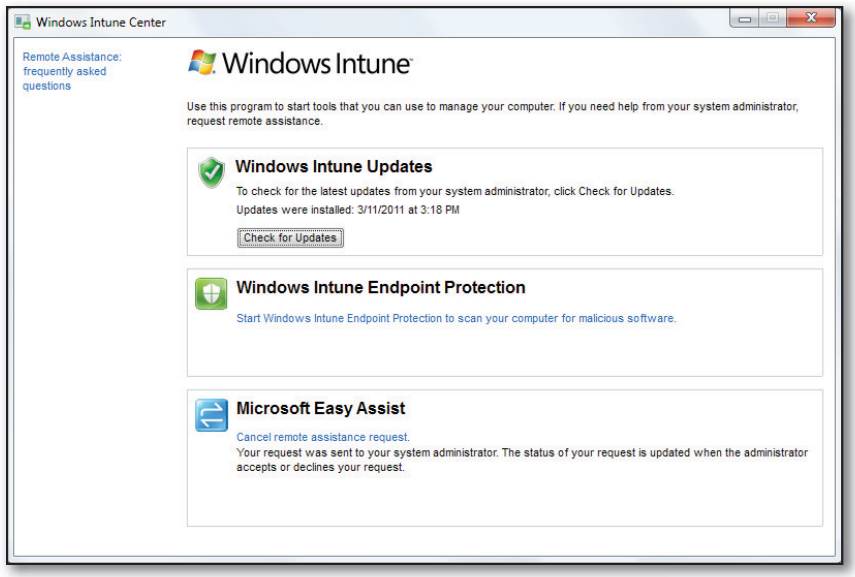


Figure 3: Windows Intune Center

Microsoft is apparently actively editing the categories list for the software inventory, so this is an area that will improve over time. That said, it's already pretty well stocked with information about all the top third-party software you'd typically find on business-class PCs, giving you a good starting point for evaluating what's out there.

License management. In the Licenses workspace, administrators who represent larger environments with Microsoft volume licensing agreements (e.g., Windows, Office) can upload agreements and ensure that they're in compliance. There's no licensing enforcement here at all, just a list of what you have and what you're using.

Intune policies. The Policy workspace is arguably the heart of Windows Intune at the moment. Although System Center and Group Policy veterans will find this interface somewhat cute, those who've never had such control over their environments might see it as an epiphany. From this simple UI, you can configure Intune policies that, again, are standalone policies that exist only for Intune-managed computers and outside of Group Policy (if you're using Group Policy in your own environment).

In that sense, Intune in general might seem like a better solution for smaller, less centrally managed environments. And although I do believe this to be the case, I find one of Microsoft's observations about Intune usage in larger environments to be compelling as well: As your employee base expands outward, with many employees working from home or on the road, and many never actually connecting to the corporate network, there's a new need for protecting these edge cases. (Some companies are even deploying Intune for executives' home machines.) Even in its first version, Intune provides an effective solution in this regard and can work alongside larger, more powerful in-house (on-premises) PC-management solutions.

In this age of consumerization in IT, more users are bringing their own PCs and devices to work; Intune is ideally suited for such scenarios.

Intune policies can also work with Group Policies. Microsoft doesn't recommend this, but the general rule is that Group Policies take precedence over Intune policies. Note, too, that Intune policies are far simpler than Group Policies, because Intune policies can be applied only at a single level: to computer groups. So there's no need (for now, at least) to worry about multiple policies contradicting each other. Policy management might get more complex in the future, as Intune matures, although Microsoft says the program has been architected to avoid this problem.

Although the policies themselves are simple enough, each policy will have a pretty extensive list of settings you control, as well as three basic templates to choose from on first creation. These templates, which include Windows Intune Agent Settings, Windows Intune Center Settings, and Windows Firewall Settings, essentially determine which entity will be affected by the settings changes contained in the policy. Templates related to the agent have dozens of settings related to Endpoint Protection and software updating, whereas those related to Windows Firewall are, as you'd expect, firewall related, with a host of possible exceptions to enable.

After you create a policy, you can manage policy deployment, which is determined on a computer group–by–computer group basis. It's a simple check-box affair.

Reporting. Windows Intune also features rich reporting functionality based around the product's various features. You can easily generate reports for updates, installed software, and licensing. Reports can be generated on the fly, then printed directly from the console or exported as an HTML or CSV file.

You can also generate reports in other parts of the administration console. For example, if you're viewing a list of alerts in the Alerts workspace or looking at the Definition Updates list in Updates, there's always a handy Export List button available.

Administration. From the Administration workspace, you can configure settings related to the administrator accounts, set category and rules classifications, configure alert types and notification rules, and manually download the client software.

The Client Experience

I installed the Windows Intune agent and associated software manually on my own client PCs, replacing the previous security solution (Microsoft Security Essentials—MSE) with Intune Endpoint Protection. (In prerelease form, Intune provided separate 32-bit and 64-bit clients, but the final version includes only one client download.) Generally speaking, using Intune Endpoint

Learning Path

***WINDOWS IT PRO* RESOURCES:**

"Is the Cloud Really Just the Return of Mainframe Computing?" InstantDoc ID 129854

"Cloud Computing 101," InstantDoc ID 129838

"Why IT Is Moving to the Cloud," InstantDoc ID 129285

"Making the Cloud a Bit Less Foggy," InstantDoc ID 128874

"Getting Smart About Cloud Computing," InstantDoc ID 126037

"The Rise of Cloud Computing," InstantDoc ID 103674

Protection doesn't affect the performance or day-to-day use of the PCs in any meaningful way. In addition, Intune Endpoint Protection looks and works much like MSE.

Intune Endpoint Protection, like FEP 2011 and MSE 2, uses heuristic-based methods to examine suspect software for new malware. And because the back end is a shared infrastructure with those other products and with System Center, customers receive the shared benefits of a large number of users, with their feedback improving accuracy across all products. I use MSE 2 on all my standalone PCs, and I recommend it highly.

Windows Intune Center, as I mentioned previously, provides a handy front end to Windows Update, Endpoint Protection, and of course the remote assistance functionality, through a feature called Microsoft Easy Assist. The benefit here is that this software works wherever you have an Internet connection; your clients don't have to be on a corporate network to get help—and indeed, many Intune end users won't ever be directly connected to your business.

Costs and Additional Benefits

Windows Intune isn't necessarily cheap: It costs $11 per PC per month. But this price also includes a licensed copy of Windows 7 Enterprise for each PC, which Microsoft says can help you maintain a bit of consistency across your environment. That's a good deal if you need it, but I'd rather see a lower price option that foregoes this client license. On the good news front, those with volume license agreements will get credit for their preexisting purchases and could thus see lower bills. (And let's give Microsoft credit here for licensing simplicity, which isn't typically the company's strong point.)

For an additional $1 per PC per month, Intune customers can also access the full MDOP suite. If you're already paying for Intune, that's a tremendous value: MDOP includes many excellent tools and utilities, such as App-V and Microsoft Enterprise Desktop Virtualization (MED-V), Microsoft Advanced Group Policy Management (AGPM), System Center Desktop Error Monitoring (DEM), Microsoft Diagnostics and Recovery Toolset (DaRT), and AIS. That said, MDOP is currently a better deal for larger companies.

These per-PC per-month pricing schemes are very common to cloud services, and like any subscriptions you pay for at home, these relatively small monthly charges can add up. For example, paying for both Intune and Office 365 could strain the resources of a typical small business. Perhaps Microsoft will eventually adopt a model in which customers who subscribe to both products get a discount as well.

> Windows Intune is a great example of what's possible with cloud services.

For now, Microsoft is preaching total cost of ownership (TCO) for these services. And in the case of Intune, the company claims that customers are saving an average of over $700 per year per PC with Intune, $520 of that from IT labor reduction and related savings. (And that's on top of the $150 to $1,400 the company's customers save per PC per year by migrating to Windows 7, depending on the starting infrastructure.)

Recommendations

Although Windows Intune will likely see its biggest successes in the high end of the small business market, as well as the midmarket—that is, organizations with roughly 50 to 1,000 PCs—this is a solution that's going to see a wide range of adoptions. The lack of true AD integration will be viewed by some as a negative, but I think this form of ad-hoc management is the future for the lower end of the market and something I'd caution Microsoft about "fixing" too quickly. In this age of consumerization in IT, more and more users are bringing their own PCs and devices to work, or at least using their own machines to perform work. And Intune is ideally suited for such scenarios.

If you have any form of corporate infrastructure, however, you'll have to undergo a process of duplicating, as much as possible, your infrastructure within Intune—and doing so gets increasingly tedious as the size of the business in question grows. But as Microsoft noted to me in a recent briefing, even the largest enterprises could benefit from using Intune on the side, as it were, to protect those machines that will never connect to the corporate network—a scenario that's becoming more and more common.

Microsoft provides a 30-day trial of Windows Intune, which you can use with up to 25 client PCs: All you need is a Windows Live ID and a collection of PCs on which to test the agent. Intune evaluation is simple and painless, and I strongly recommend it.

Looking ahead, Microsoft plans to update Intune on a regular basis and is already talking, somewhat generally, about plans for future releases. The company expects Intune to match the current level of System Center management functionality within 2 to 3 years, for example, and will more specifically be improving the product to include software deployment in a coming release.

Microsoft's plans for Windows Intune are all very exciting. But even in its first version, Intune is a great example of what's possible with cloud services, and the product provides a great solution for companies that fall within its sweet spot.

InstantDoc ID 129945

Paul Thurrott
(thurrott@windowsitpro.com) is the senior technical analyst for *Windows IT Pro*. He writes a weekly editorial for *Windows IT Pro UPDATE* (www.windowsitpro.com/email) and a daily Windows news and information newsletter called *WinInfo Daily UPDATE* (www.wininformant.com).

THE CONVERSATION BEGINS HERE

SharePoint CONNECTIONS Coast to Coast Tour + Microsoft SharePoint BOOTCAMP

COMING TO A CITY NEAR YOU IN 2011!

DIVE INTO SHAREPOINT 2010 WITH MICROSOFT AND SHAREPOINT INDUSTRY EXPERTS.

Register now for the developer and IT pro bootcamps. **SPACE IS LIMITED!**

EARLY BIRD fee: $499

REGULAR fee: $599

REGISTER EARLY

The first 100 developers to register for the ***SharePoint Coast-to-Coast Tour*** in each city get into the hands-on *Microsoft SharePoint 2010 Development Bootcamp* for **FREE**!

A SAMPLING OF SPEAKERS

MICHAEL NOEL
CONVERGENT COMPUTING

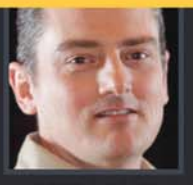
STEVE FOX
MICROSOFT

DAN HOLME
INTELLIEM, INC.

RICHARD TAYLOR
PERFICIENT

TODD BAGINSKI
FRESH TRACKS CONSULTING, LLC

MATT MCDERMOTT
ABLEBLUE



SCOT HILLIER
SCOT HILLIER TECHNICAL SOLUTIONS, LLC

ASIF REHMANI
SHAREPOINT ELEARNING.COM

CHRIS GIVENS
ARCHITECTING CONNECTED SYSTEMS

PAUL STUBBS
MICROSOFT

DARRIN BISHOP
KNOWLEDGELAKE, INC

ROBERT L. BOGUE
THOR PROJECTS

ANDREW CONNELL
CRITICAL PATH TRAINING, LLC

RANDY WILLIAMS
SYNERGY CORPORATE TECHNOLOGIES

TO REGISTER: DevConnections.com/SPTour 800.438.6720

Mark Russinovich Discusses Windows Azure

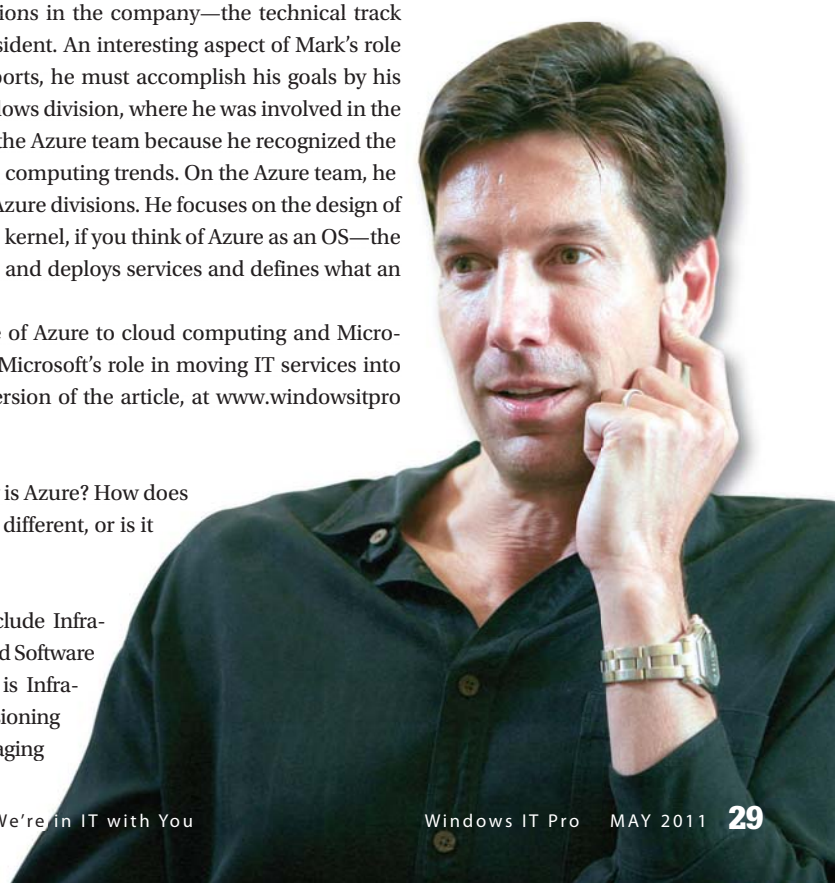
Microsoft dives deep into the cloud

by Sean Deuby

Cloud computing is a very popular topic, but when I ask most IT professionals to explain it, I always encounter varying degrees of confusion. This confusion is even prevalent regarding Azure, Microsoft's cloud computing platform. Because Azure fits into the middle tier of the cloud computing service model—Platform as a Service (PaaS)—it's very developer focused, rather than IT pro focused. This doesn't mean, however, that cloud computing won't be vitally important for IT pros to understand for their future. In an effort to help explain what Microsoft is doing in cloud computing, I sat down at Microsoft's 2011 MVP Global Summit with *Windows IT Pro* contributing editor, Microsoft technical fellow, and old friend Mark Russinovich to have him explain what Windows Azure is and how it's important to Microsoft's future.

Well-known among IT pros as the OS researcher who developed unique utilities for Windows by reverse-engineering the Windows OS, Mark joined Microsoft in 2006 when the company purchased his Winternals software company. As one of only 20 technical fellows throughout Microsoft, Mark occupies one of the highest individual contributor positions in the company—the technical track equivalent of the management track's corporate vice president. An interesting aspect of Mark's role as a technical fellow is that because he has no direct reports, he must accomplish his goals by his considerable influence alone. After moving from the Windows division, where he was involved in the planning of Windows 7 and its successor, Mark moved to the Azure team because he recognized the growing importance of both cloud computing and mobile computing trends. On the Azure team, he works with team leaders, as well as developers in various Azure divisions. He focuses on the design of the fabric controller, which Mark describes as "the [Azure] kernel, if you think of Azure as an OS—the kernel, which knows how to manage the server hardware and deploys services and defines what an Azure application is."

Let's see what Mark had to say about the importance of Azure to cloud computing and Microsoft, where he sees the cloud heading in the future, and Microsoft's role in moving IT services into the cloud. (For the complete interview, see the online version of the article, at www.windowsitpro.com, InstantDoc ID 129988.)



Sean Deuby: From the IT pro's point of view, what exactly is Azure? How does it fit in with Microsoft's other online properties? Is it truly different, or is it just another "Live" service?

Mark Russinovich: Cloud computing service models include Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). What you've seen IT pros focus on is Infrastructure as a Service. So in their own data centers, provisioning servers, provisioning applications on those servers, managing

them, monitoring them—Infrastructure as a Service is on-demand multi-tenant access to infrastructure resources.

Canonical examples include Amazon EC2, VMware, and Hyper-V. Those kinds of infrastructure clouds or virtualization platforms let you basically rent someone else's server and deploy your OS and applications to that server—but other than that, those platforms try to look as closely like your data center as possible, to make it easy to just take your apps, lift them up, put them there, and as much as possible use the same management that you use to manage your on-premises data center applications.

There's fidelity loss when you're going to a public cloud like Amazon's EC2. There's higher fidelity when you go to a private cloud like VMware vCloud that providers such as Rackspace would provide. Or if someone else is hosting a Hyper-V cloud, you also get high fidelity. What PaaS tries to do is raise the level of abstraction up one level.

The benefit of taking it up a level from an IT pro perspective and from a business perspective is that you're not now in the business of worrying about provisioning the OS, provisioning of the runtimes, and provisioning the database and the other infrastructure services that these traditional server applications use or are built on. The benefit from a developer's perspective is that you don't have to worry about any of that stuff.

On top of that, the platform makes it really easy to write a cloud or a 24 × 7, highly available, highly elastic application. That's what Azure is about—and PaaS from an Azure perspective for the compute part of it makes it almost brain-dead simple to write an app that's multi-tier, multi-instance, and has this ability to scale up and down very quickly and be able to stay up 24 × 7 even in the face of hardware failures or configuration updates, or updates of the service to new versions.

Sean: Doesn't Azure also support coexistence, meaning the ability to have a hybrid application that's partly on premises and partly in the cloud?

Mark: Yes. Just to finish discussing PaaS, there's compute PaaS, which is what Azure has, and then there's the building-block Platform as a Service, which is all the other services that cloud applications will use to implement functionality for it. If you look at on-premises server applications, a lot of times they have a database back end—which is stood up with a SQL Server instance or pair of instances if you want high availability on the data center. With a cloud, looking at a cloud application, it's using the same kind of PaaS building blocks to provide that functionality; in this case it would be SQL Azure. And the characteristics I talk about for compute cloud applications—24 × 7, highly available, highly elastic—apply to those as well. And you pay only for what you use, rather than overprovision, which is another big problem that on-premises has.

This is the problem where if you're building your own data center and you're deploying your apps to it, to determine how much hardware you need, you look at the app and ask, "What's the maximum load this app is going to have?" Around Christmas, it's like 100 times what it is normally, so we need 100 times the hardware that we do for everyday operations. And in the cloud, it's because of this pay-as-you-go, highly elastic nature, you pay for the 1 percent you use on a daily basis, and around the holidays you scale it up to 100 times and you pay for that for the time that you need it. Then you just go back down afterwards, instead of having all this wasted capacity.

From an IT pro perspective, this composite type of application—the hybrid application—becomes interesting in the case where, for the most part, I want to run my applications on premises, but around the holidays, when I've been paying for 1 percent and I'm monitoring things closely, I want to burst into somebody else's cloud so that I can take advantage of that elasticity and pay for it only right when I need it, and then come back down into my own—we see customers that are really interested in that type of scenario.

Sean: So it's a conservative way to get your feet wet on public cloud services. You design an application for likely usage—you don't have to design for maximum capacity, you design for average capacity, and you have a fail-safe off to the cloud for maximum capacity.

Mark: Yes. What we're talking about is future scenarios that will be enabled by the Windows Azure appliance. The other scenario is hot standby for disaster recovery, where you've got the standby of the application up in somebody else's data center in the cloud, and you've got the active one on premises, but you fail over if there's a problem with the on-premises one. The app is running in the cloud but then talking to resources back on premises, which is something that's enabled today (with Windows Azure Connect, which lets you actually domain-join the machines in the cloud and also have access to on-premises network resources, basically making them appear as if they're on your intranet). So Windows Azure public cloud applications can access your on-premises SQL Server database, for example. If you still have lots of data on premises, or data that you don't want to leave your premises, that connectivity allows this kind of hybrid connection between on-premises stuff and cloud stuff.

Sean: You mentioned Infrastructure as a Service and PaaS. Do you want to say anything about SaaS?

Mark: Azure started out as a platform aimed at internal services only, but once people saw it, they realized, "Hey, we could actually deliver this to the outside world, and they'd probably find it useful and interesting as well." Windows Azure has become an extremely important platform for Microsoft, because Microsoft is planning to build lots of SaaS offerings (such as Office 365)—but what are they going to build them on? They're going to build them on Windows Azure, so Azure is important for that aspect of the business as well. But as a Platform as a Service, it's really a platform for SaaS—for building Software as a Service. If you look at an IT pro ISV scenario—a guy writing line-of-business applications—that's really SaaS, to some extent. It's a cloud application. But it eventually enables the ability of other people that create these multi-tenant cloud applications that they're then selling to IT pros.

Sean: So in other words, Microsoft is itself using Azure to build SaaS applications that are the service-enabled versions of the enterprise software you're selling today.

Mark: Exactly. Actually, that explanation highlights the kind of transition Microsoft is going through right now.

Sean: How important is Azure to Microsoft?

Mark: Microsoft's new philosophy is "cloud first," and then ship what we deliver to the cloud in the on-premises box solution, because there's something drastically different between the way the cloud works and the way that on-premises server software works. On-premises server software is the traditional box model—I get an update every 2 years. And I might hop on that update bandwagon every release, or I might skip a release or two because the old one was good enough for awhile.

But the cloud is shipped every month. What's going on with Windows Azure is that we're shipping every month. There's a new version of the fabric controller rolled out across all our data centers once a month. All of the other cloud properties are in the same kind of cadence. New features, major features, might only surface once every 6 months or at some longer cadence. Every one of these incremental updates is fixing bugs and introducing the pieces required to create the functionality that's going to end up surfacing as a feature that we sell to customers or make available to customers. So it makes total sense for us to say that the cloud will be so important, and we'll be delivering updates so frequently to cloud-based applications, that updates to the box product will be snapped off the cloud version at regular intervals.

You can see that happening with the SQL Server team. SQL Azure is off in a cloud—it shares the same core with SQL Server, so as the cloud evolves, the result of that evolution is going to make it back into SQL Server for the on-premises version.

You're probably going to see all ISVs follow this same model.

Sean: Is the fabric controller that you're working on going to be used as a platform to connect Microsoft SaaS products?

Mark: Yes. For example, System Center will eventually have multiple components that run in the cloud. Windows Intune, which is the client-focused System Center management solution, runs in the cloud. And upcoming System Center cloud-based components will be built on the Windows Azure fabric. So these components will take advantage of PaaS, but they're really SaaS.

Sean: So you're building SaaS based on PaaS, which means there's probably some Infrastructure as a Service going on too.

Mark: Today, Infrastructure as a Service means compatibility with server applications. We've got a new programming model in Windows Azure. Typically, most server applications don't fit that programming model, so you need to have a developer tweak them.

Sean: Part of what makes working on the fabric controller interesting is the scaling of it, where you've described it as being analogous to the Windows kernel and controlling resources. So whereas the Windows kernel is the microscopic version, the fabric controller is the macroscopic version. Do you have anything to relate, as far as the scale at which you're working?

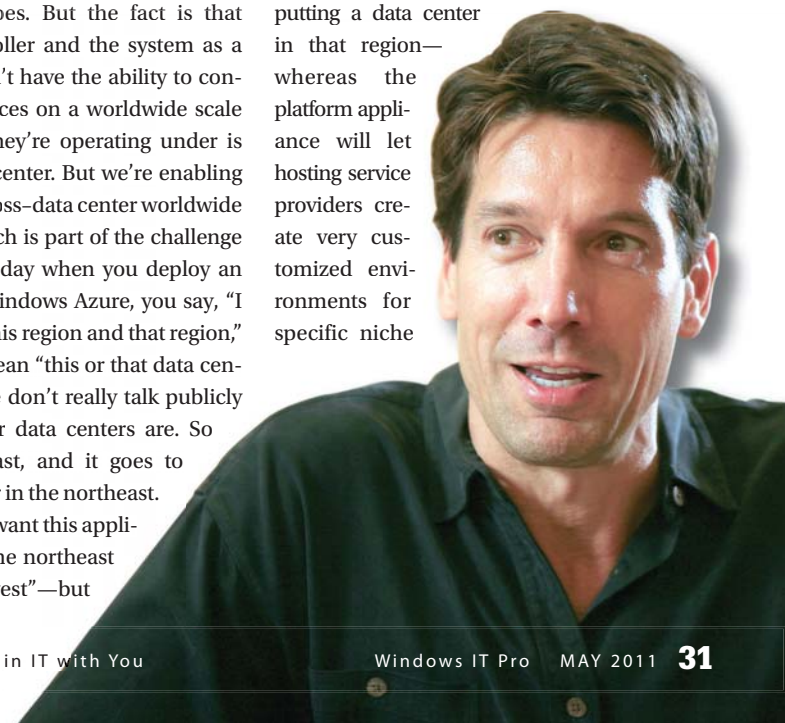
Mark: The data centers have literally on the order of tens of thousands of machines, and we're operating on hundreds of petabytes of storage.

Sean: And the fabric controller has to be able to seamlessly and efficiently deal with all of that?

Mark: Yes it does. But the fact is that the fabric controller and the system as a whole today don't have the ability to control these resources on a worldwide scale yet. The scale they're operating under is within the data center. But we're enabling those kinds of cross–data center worldwide capabilities, which is part of the challenge of growing it. Today when you deploy an application to Windows Azure, you say, "I want it to be in this region and that region," but you really mean "this or that data center," although we don't really talk publicly about where our data centers are. So you say northeast, and it goes to some data center in the northeast. You can't say, "I want this application to be in the northeast and the southwest"—but one day you will be able to. Or you'll be able to say, "Run a hot one in the northeast and have a standby in the southwest—or if it's going to be in the northeast but if it grows, it can grow into other regions as well." We still have to have people specify which regions they can run in, because there are all sorts of legal, compliance, and government issues.

Sean: Can you talk about the importance of on-premises virtualization versus putting everything out in the cloud? Some people say to put it all out in the cloud; some people say to virtualize locally.

Mark: That's something I haven't really touched on—the Windows Azure platform appliance, which is a key part of the Azure strategy. This is the ability to take Windows Azure—the hardware that it runs on and the software—and put it in your own data center. Or to have a hosting service provider take it and put it in their data center and then sell it to customers. I think that's a huge differentiator for us—the fact that we're going to have this ability because it extends the reach of the platform to anywhere people want it, whereas today, the public cloud is only acceptable to people when it just happens to meet their requirements, because their requirements are very general. The public cloud is addressing kind of the generalist case, like the most generally sought-after certification, or the geographic regions where we have a huge market that justifies putting a data center in that region—whereas the platform appliance will let hosting service providers create very customized environments for specific niche



markets, like following certain certifications and government requirements.

Sean: Is this private cloud in a box?

Mark: It's PaaS in a box, because it's different from the VMware cloud, which you can put on premises, which is an infrastructure (IaaS) cloud. Or Hyper-V, which you can put on premises and run with System Center and it's kind of like your private cloud. There's actually a difference between buying the appliance and putting it on premises, versus sharing an appliance on a hosting service provider with other customers—the former makes it kind of non-cloudish because you're paying for the whole appliance. You have a block of capacity rather than having elastic capacity. You lose that when you go away from a multi-tenant model. The hosting service provider can provide a multi-tenant model even in the kind of situation in which they're addressing the niche markets that have these unique requirements—maybe it's just for the UK government—but different departments in the UK government can now buy elastic capacity out of this sort-of-semi-public cloud.

Sean: So it's public PaaS compared with private PaaS—whereas VMware's would be more private Infrastructure as a Service.

Mark: Yes, if VMware made an appliance or someone sold the VMware appliance as private Infrastructure as a Service. Until now you've heard *public cloud* and *private cloud*. What people mean when they say public cloud is Windows Azure or Amazon; when they say private cloud it means System Center Virtual Machine Manager cloud or VMware cloud—that distinction, that way of drawing those lines, is going to go away, and it's just going to become Windows Azure wherever you want it, and whatever anybody else does.

Sean: Do you mean that the distinction between private and public cloud is more differentiated by the vendor in this case because it's designed to seamlessly interact between public and private—meaning that it's a hybrid cloud?

Mark: Yes. That's one of the design principles of the Windows Azure appliance—it's running the same software that runs in the appliance as can run in the public cloud. The other way might not be the case because the private appliance that someone's managing—they might not update it at the same time we update the public cloud. They might be at N-1; so if they want to take advantage of the features in N, they have to upgrade to N (the same version). But the cloud will always be able to run whatever runs in the appliance, to enable the bursting scenario.

InstantDoc ID 129988

Sean Deuby
(sean@windowsitpro.com) is technical director for *Windows IT Pro* and *SQL Server Magazine* and former technical lead of Intel's core directory services team. Sean has been a directory services MVP since 2004.

Recover from Active Directory Disasters

How to restore DCs and AD objects

by Brian Desmond

Active Directory (AD) is typically a key network service in any organization. Without it, everything comes to a grinding halt. With this in mind, it's important to be prepared for the various disasters that might strike a forest.

When it relates to AD, the scope of the disaster can vary quite a bit. It can be as simple as the failure of single domain controller (DC) or the accidental deletion of a single object. An even worse situation is when an entire organizational unit (OU) hierarchy is accidentally deleted. In the worst-case scenario, an entire domain or forest might need to be restored.

The good news is that many of the techniques that apply to recovering from simple disasters also apply to recovering from catastrophic disasters. I'll discuss how to recover from the two most common calamities: a failed DC and accidentally deleted objects.

Backup Strategy

You first need to make sure that you have something to use for a recovery. At a minimum, you should have valid system state backups of at least two DCs in each domain in your AD forest. Windows Server Backup (Windows Server 2008 and later), NTBackup (Windows Server 2003 and Windows 2000 Server), and most commercially available backup tools can perform valid system state backups. However, it's always worth testing the backups to make sure everything is in order. One important point regarding backup tools is that you should use a Volume Shadow Copy Service (VSS)–aware backup tool. Backup tools that rely on disk imaging or virtual machine (VM) snapshot technologies are generally incompatible with AD. Restoring a backup made by one of these tools can cause serious replication failures known as update sequence number (USN) rollback.

In many organizations, the responsibility for server backups and restores falls to a different team than the team that runs AD. This leads to a couple of problems. First, you have no direct control over the backup process, which makes validating backups difficult. Second, many backup tools require an agent on each DC being backed up, a situation that indirectly provides elevated access to the DC.

To mitigate these problems, I frequently employ a two-tiered approach to DC backups. I use a script to run Windows Server Backup each night on the DC and keep a week or two of backups locally on the DC. The folder containing the backups is then shared, with access restricted to the backup tool, as many backup tools can back up a file share without an agent. I also sometimes store the backup files on neighboring DCs within a site. So, for example, if you have DC1 and DC2 in a site, the backups of DC1 are stored on a file share on DC2 and vice versa.

The benefits of this two-tiered approach include the following:

- You mitigate some of the risk of being dependent on another team for backups.
- In the event you need to perform a restore, you can proceed right away with the native backup files you have on hand isntead of waiting for another team to perform the restore.

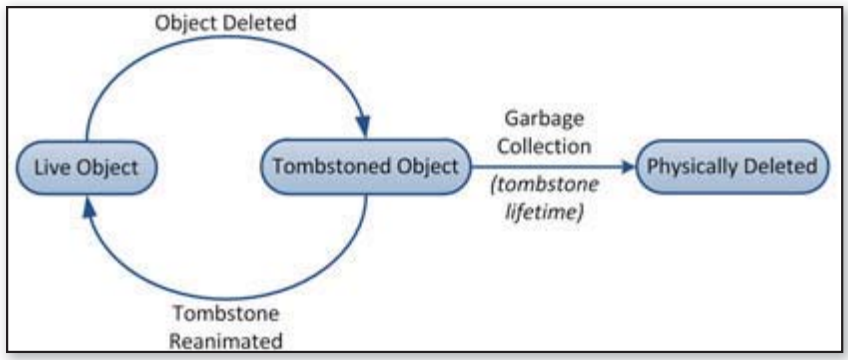


Figure 1: Default life cycle of an AD object

- You're not waiting for a backup to copy over the WAN from another site in the event backups are performed remotely.

I posted the script I use to run Windows Server Backup as well as directions for setting it up in my blog at briandesmond.com/blog/managing-local-backups-with-windows-server-backup/.

DC Recovery

A great thing about AD is the mostly stateless nature of the DC. Aside from potentially holding one or more Flexible Single-Master Operation (FSMO) roles, a DC should generally be a matching replica of other DCs in the domain, except for some potential delay in replication depending on topology. If a failure renders a DC inoperable, this stateless nature is fantastic because it will often remove the need to go through a complicated restore from a backup. Instead, you can simply reinstall Windows and use Dcpromo to promote the server to a DC and replicate all of the data back in—assuming your domain has more than one DC. If you have only one DC in your domain, you can greatly reduce your exposure to failure by deploying a second one.

Before you reinstall and repromote a DC, though, you need to clean up AD, which is a two-step process. The first step is to seize any FSMO roles that the DC might hold for another DC in the domain. If you're not sure which DCs are hosting FSMO roles in the domain, run

```
netdom query fsmo
```

in a command prompt window to find out. You can then seize the FSMO roles using the Ntdsutil utility. Follow the instructions under the *Seize FSMO roles* section in the Microsoft article "Using Ntdsutil.exe to Transfer or Seize FSMO Roles to a Domain Controller" (support.microsoft.com/kb/255504). When you seize an FSMO role, best practice is to never bring the original role-holder back online.

Because the original FSMO role-holder can't go back in service, the second step is to clean up the metadata of the failed DC's configuration in AD. You can use Ntdsutil for this step. Follow the steps in the Microsoft article "How to Remove Data in Active Directory After an Unsuccessful Domain Controller Demotion" (support.microsoft.com/kb/216498). Alternatively, if you're using the Server 2008 (or later) version of the Active Directory Users and Computers snap-in, you can complete this step by deleting the DC's computer account in the Domain Controllers OU.

Repromoting a DC over the network might not be feasible when the amount of data to replicate would strain the network. In this case, there are a couple of other options. The first option is to restore the DC's system state from a backup and continue on. The second option is to use the Install from Media (IFM) functionality, which was added in the Windows 2003 release. IFM lets you take a system state backup (created with NTBackup in Windows 2003) or IFM media (created with Ntdsutil in Server 2008 or later) and point Dcpromo to the AD database in the IFM media. IFM media created by Windows 2003 must first be restored to an alternate location on the file system so that Dcpromo can consume it. The DC will make the necessary changes to the database in the media and replicate only the changes since the media was created over the network.

AD Object Life Cycle

Deleting an object doesn't directly correlate to a record being removed from the AD database. To maintain consistency in AD's replication model, objects first transition through a state known as being tombstoned, as Figure 1 shows. Rather than implementing a distributed mechanism to replicate physical deletions from the database, AD replicates a change to an attribute that indicates the object has been deleted.

When you delete an object from AD, the isDeleted attribute is set to True, which means nearly all the object's attributes are removed. The object is moved to the Deleted Objects container, and its lastKnownParent attribute is stamped with the distinguished name (DN) of the parent object before the object is deleted. After an object has been marked as deleted, it won't be visible to any tools that query AD, unless you add a special LDAP control to indicate that you want AD to return deleted objects in the search results. Various free LDAP query tools (such as AdFind from www.joeware.net) include this LDAP control.

At this point, the object will remain as a tombstone for a period of time. The default tombstone lifetime for forests is based on the OS of the first DC in the forest. Table 1 shows the default tombstone lifetimes. Upgrading AD doesn't change the tombstone lifetime for the forest.

Periodically, a background process called garbage collection runs on each DC. The garbage collector scans the database for tombstones that are older than the forest's tombstone lifetime and purges them from the AD database.

Until the point when a tombstone is purged by the garbage collector, you can recover the object using tombstone reanimation. When you reanimate a tombstone, you only get back a handful of attributes that are kept during the tombstoning process. For example, the attributes saved for a user object include the user's SID,

Table 1: Default Tombstone Lifetime for New Forests

First DC's OS	Tombstone Lifetime
Windows 2000	60 days
Windows 2003	180 days
Windows 2003 R2	60 days
Server 2008	180 days
Server 2008 R2	180 days

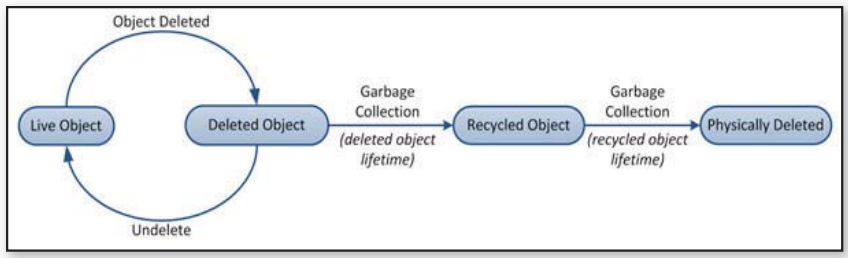


Figure 2: Life cycle of an AD object when the Active Directory Recycle Bin is enabled

SID history, and username (sAMAccountName). Notice that this list doesn't include attributes such as the user's password, group membership, or demographic information (e.g., name, department). You can control the list of attributes that are preserved when an object is tombstoned by modifying the searchFlags attribute of an individual attribute's definition in the schema. You can add as many attributes as you like. However, you can't add linked attributes, such as group membership or the mailbox database containing a user's mailbox.

In AD forests operating at the Server 2008 R2 forest functional level (FFL), you can enable the new Active Directory Recycle Bin. As Figure 2 shows, the Active Directory Recycle Bin adds an intermediate state between when an object is deleted and when it is tombstoned. When an object is in this new deleted state, it's hidden from search results but all its attributes (including linked attributes such as group membership) are preserved.

An object in the deleted object phase can be recovered to the exact state it was in at the time of deletion using the same process that's used to reanimate a tombstone. By default, an object stays in the deleted object phase for the same amount of time as the forest's tombstone lifetime, as outlined in Table 1. You can change this time period by modifying the forest's msDS-deletedObjectLifetime attribute.

After the deleted object lifetime expires, the garbage collector moves the object into the recycled object phase. A recycled object is the functional equivalent of a tombstone, with one difference: You can't reanimate a recycled object or restore it from backup.

Object Recovery Mechanisms

As AD has matured from release to release, the mechanisms to recover a deleted object have evolved significantly. In Windows 2000, the only way to get a deleted object back was to perform an authoritative restore from a backup. Windows 2003 introduced the concept of tombstone reanimation, which lets you get a partial copy of the deleted object back without restoring it from a backup. Server 2008 R2 added the Active Directory Recycle Bin, which allows the complete recovery of a deleted object without a restoration.

It's imprtant to note that the shelf lifetime of an AD backup (as well as IFM media) is the same as the tombstone lifetime. If you have the Active Directory Recycle Bin enabled, the shelf lifetime is the lesser of the deleted object lifetime or recycled object lifetime. For example, if the deleted object lifetime is 180 days and the recycled object lifetime is 60 days, then the shelf lifetime is 60 days. Thus, it isn't possible to restore a deleted object from a backup that's older than either of these values.

Authoritative Restore

When you need to get an object or series of objects back from a backup, the authoritative restore process is often the way to go. If you've ever wondered what the Directory Services Restore Mode (DSRM) option on a DC's F8 boot menu is for, this is the option you choose to perform an authoritative restore. When you boot in DSRM mode, AD is never started and the database is offline. You can restore the AD database from a backup while booted into DSRM mode, then use Ntdsutil to select the objects that need to be restored. Note that it isn't possible to perform a restore when the AD NTDS service is stopped on Server 2008 and later DCs.

When you perform an authoritative restore, AD increments the internal version number of the objects being restored. This ensures that when the DC is back online, those objects are replicated out into the rest of the domain and the restored version becomes globally effective.

Authoritative restores are often performed to recover OUs that contain a large number of objects (e.g., users, groups, computers, other OUs). Suppose that you accidentally deleted the Executives OU from the contoso.com domain. To get the OU and everything in it back, here are the steps you need to take:

1. Boot into DSRM mode and log on with the DSRM password you set during Dcpromo.
2. Restore a system state backup that was created before the accident. Don't reboot. (This is a common mistake, especially when under pressure.)
3. Launch a command-prompt window and run Ntdsutil.
4. Run the command

```
authoritative restore
```

5. Run the command

```
restore subtree
  OU=Executives,DC=contoso,DC=com
```

6. Review and confirm the confirmation safety prompts. You should then receive a message like the one in Figure 3. Make note of the text and LDAP Data Interchange Format (LDIF) files that are generated.
7. Reboot the DC into normal operating mode.

```
Successfully updated 72 records.

The following text file with a list of authoritatively restored
objects has been created in the current working directory:
     ar_20110221-151131_links_contoso.com.txt

One or more specified objects have back-links in this domain. The
following LDIF files with link restore operations have been
created in the current working directory:
     ar_20110221-151131_links_contoso.com.ldf

Authoritative Restore completed successfully.
```

Figure 3: Message noting a successful authoritative restore

```
Enumerating domain deleted objects:

cn: John Doe
DEL:c7aee04d-709b-4e79-a190-148c532a99c8
distinguishedName: CN=John Doe\0ADEL:c7aee04d-709b-4e79-a190-
148c532a99c8,CN=Deleted Objects,DC=contoso,DC=com
lastKnownParent: OU=Test Users,DC=contoso,DC=com

Found 1 item matching search criteria.
```

Figure 4: Sample output from the AdRestore utility

8. Log on to the DC and open a command-prompt window. Import the LDIF file exported during step 6 by running the command

```
ldifde -i -f
  ar_20110221-151131_links_contoso
    .com.ldf
```

This will import the linked attribute values (such as group membership) for the objects restored.

If you need to restore only a single object (e.g., a deleted computer object), you can use the *restore object* command instead of the *restore subtree* command in step 5. If your forest contains multiple domains, you need to use the text file exported in step 6 to restore group membership for domain local groups in other domains.

Tombstone Reanimation

There are a number of tools that you can use to reanimate a tombstone, but they all ultimately perform the same steps. So, as an example, here are the steps you need to take to reanimate a deleted user named John Doe with the AdRestore utility (technet.microsoft.com/en-us/sysinternals/bb963906):

1. Open a command-prompt window and search for the user with the command

```
adrestore Doe
```

AdRestore will search the deleted objects for anything matching *doe* and return output like that in Figure 4.

2. Make sure the object you want to reanimate is present, then run AdRestore again with the -r switch:

```
adrestore -r Doe
```

3. Confirm the prompt asking if you want reanimate the object. AdRestore will then reanimate the object to the location it was previously found.

As I mentioned, tombstones lose most of their attributes upon deletion. So, you'll have to repopulate many of the attributes to make the reanimated object useful again.

Active Directory Recycle Bin Undelete

The Active Directory Recycle Bin is undoubtedly the best recovery option because all attributes are restored, including linked attributes such as group membership. However, as mentioned previously, your forest needs to be operating at the Windows Server 2008 R2 FFL to take advantage of it.

You can use Windows PowerShell to enable the Active Directory Recycle Bin by running a command such as

```
Enable-ADOptionalFeature -Identity
  'CN=Recycle Bin Feature,
  CN=Optional Features,
  CN=Directory Service,
  CN=Windows NT,CN=Services,
  CN=Configuration,DC=contoso,DC=com'
  -Scope ForestOrConfigurationSet
  -Target 'contoso.com'
```

Note that enabling the Active Directory Recycle Bin is not a reversible step. In addition, objects that are already tombstoned when you enable the Active Directory Recycle Bin will no longer be recoverable through tombstone reanimation.

After you've enabled the Active Directory Recycle Bin, any objects that are subsequently deleted will be recoverable in their entirety for the duration of the forest's deleted object lifetime. There are a number of ways to undelete objects, but the easiest is to use PowerShell's Restore-ADObject cmdlet. For example, here are the steps to undelete a user named John Doe:

1. Launch the Active Directory Module for Windows PowerShell from the Administrative Tools section of the Start menu.

2. Search for the deleted user by running the command

```
Get-ADObject -SearchBase
  "CN=Deleted
    Objects,DC=contoso,DC=com"
  -ldapFilter:"(msDs-lastKnownRDN=John
    Doe)"
  -IncludeDeletedObjects
  -Properties lastKnownParent
```

Make sure that it's the only object returned in the result set.

3. Restore that object with the command

```
Get-ADObject -SearchBase
  "CN=Deleted
    Objects,DC=contoso,DC=com"
  -ldapFilter:"(msDs-lastKnownRDN=John
    Doe)"
  -IncludeDeletedObjects
  -Properties lastKnownParent |
  Restore-ADObject
```

If you deleted an entire OU, you'll need to recover objects in the correct order (i.e., such that an object is not recovered before its parent is recovered) so that they can be put back where they belong. Microsoft has posted a tree undelete PowerShell script that you can use to perform this task at technet.microsoft.com/en-us/library/dd379504(WS.10).aspx.

A Complex Task

Planning for an AD disaster is a complex task because of the multitude of things that can go wrong. However, if you know how to recover from a failed DC and the accidental deletion of an object or an entire tree of objects (such as an OU), you're well on your way to being prepared for a disaster.

InstantDoc ID 129989

Brian Desmond
(brian@briandesmond.com) is a Directory Services MVP and senior consultant for Moran Technology Consulting in Chicago. Brian is author of *Active Directory, 4th Edition* (O'Reilly).

Deciphering PKI

How encryption, digital signatures, and digital certificates work

by Russell Smith

Many systems administrators are turning to public key infrastructure (PKI) solutions as the trend of letting data flow freely past network boundaries becomes more prevalent. Most people associate PKI with encryption, but PKI isn't just about encryption. It's also about data integrity and authentication. So, before implementing a PKI solution, you need to understand how encryption, digital signatures, and digital certificates work together to secure and maintain the integrity and confidentiality of sensitive data.

Encryption

Encryption is the process of turning legible clear text, which is referred to as plaintext, into incomprehensible ciphertext. In other words, you use cryptography to make the data you want to keep secret indecipherable to everyone except for the people with the necessary key to decrypt it.

Cryptography uses mathematical methods, sometimes referred to as ciphers or algorithms, to scramble data so that it can't be easily read without the necessary key. A decryption key is usually a long random number that you must possess to decrypt a given piece of data using the same algorithm with which the data was encrypted.

There are several types of encryption, including symmetric and asymmetric. In symmetric encryption, shared keys are used to encrypt and decrypt data. The encryption and decryption keys can be identical or one key can be easily derived from the other. Although symmetric encryption is computationally fast, it requires that the key be exchanged between the sender and recipient. If the key is compromised during transit, the encrypted data can be read by the person in possession of the key.

Asymmetric encryption, which PKI implements, involves two keys: a public key and a private key. As Figure 1 shows, the process starts when a sender uses a public key to encrypt a message. The sender can request a public key from the intended recipient or download it from a public directory or website. Only the intended recipient can decrypt the message with its corresponding private key. Although slower than symmetric encryption, asymmetric encryption doesn't require a secure key exchange.

Symmetric and asymmetric encryption are often used together. An asymmetric cipher is used to encrypt a session key (i.e., a symmetric key intended for use in a given exchange of data), and the encrypted session key is used to encode the message. This approach, which is referred to as bulk encryption, provides the security of asymmetric encryption with the speed of a symmetric cipher.

The length of the key is an important factor in bulk and asymmetric encryption. It's mathematically feasible to derive a private key having access only to a public key. Therefore, as computing power constantly improves, you should assume that the encrypted data will be secure for only a limited amount of time. The longer the key, the more time your data should remain secure. However, longer keys are more processor intensive, so you need to strike a balance between security and speed.

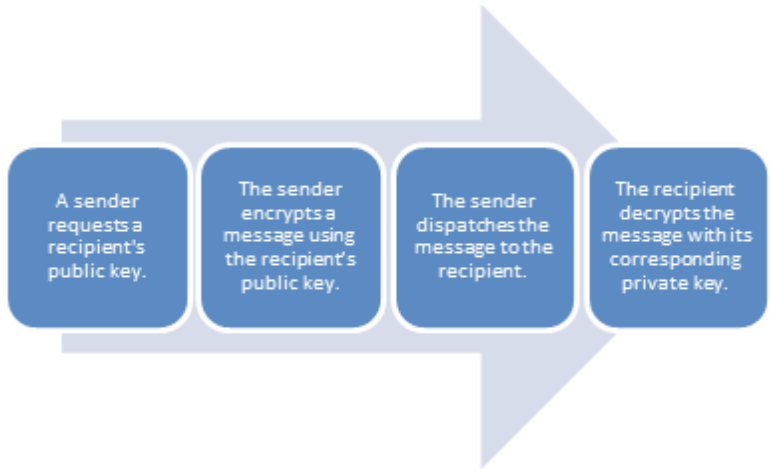


Figure 1: Asymmetric encryption process

The length of a shared key is also an important factor in symmetric encryption. For information about the key lengths in symmetric and asymmetric encryption standards, see the web sidebar "Common Encryption and Hash Standards" (InstantDoc ID 129847).

Digital Signatures

Public key cryptography can be used to issue messages with a digital signature. As with a handwritten signature, this seal of approval enables a message's receiver to verify that the information did in fact come from a given sender. Digital signatures are much more reliable than handwritten signatures, as it's very difficult to produce a fake digital signature. In addition, the integrity of the message content is guaranteed.

A hash is used to ensure message integrity—in other words, it guarantees that the message hasn't been modified in transit. Hash algorithms analyze a message, then generate a small code (hash or message digest) that uniquely identifies it. Changing a message without changing its hash is difficult. Besides proving that a message hasn't been modified, hash algorithms ensure that no two messages have the same hash.

Hash algorithms produce message digests that form part of the digital signature sent with a message. As Figure 2 shows, the process begins when the sender uses an algorithm to generate a hash of the original data to form a message digest. The sender then uses its private key to encrypt the message digest and sends the message to the recipient. The recipient generates its own hash of the message using the same algorithm. The recipient decrypts the original message digest sent with the message using the sender's public key and compares the two digests. If they're identical, the message hasn't been tampered with in transit.

You can't easily use self-signed certificates to authenticate the identity of internal resources or devices outside of your organization.

Digital Certificates

Digital certificates are electronic documents that contain:

- A public key
- Information about the purposes for which the certificate can be used (e.g., server authentication, email encryption)
- Start and end validity dates
- Identity information about the individual or organization using the certificate
- A digital signature to attest that the identity information provided corresponds with the included public key

Digital certificates are usually distributed in the standard X.509 format.

A Certification Authority (CA) is a trusted entity that confirms the identities of individuals and organizations that are using digital certificates, much in the same way that one government relies on the passport authority of another country to validate its citizens' identities. For instance, if you require a digital certificate for a public-facing web server for data encryption and server authentication, you can approach a CA to confirm your organization's identity and send information that only your company can provide. Client OSs usually come supplied with the root CA certificate of the most commonly used public CAs (e.g., Thawte, VeriSign), enabling the OS (and the applications that run on it) to trust them. If you require authentication inside your organization only, you can install and manage your own CA.

CA systems consist of several components, including a registration authority and a validation authority. The registration authority is responsible for proving the identity of entities that require a certificate. It's also responsible for revoking certificates, approving requests to renew expiring certificates, and providing a new key for an existing certificate (i.e., re-key a certificate).

The validation authority is used to provide real-time assurance that a certificate is valid. This can be done by checking certificate revocation lists (CRLs) or using the Online Certificate Status Protocol (OCSP), which I'll discuss shortly. First, though, I want to bring up the topic of self-signed certificates.

Because public keys for asymmetrical encryption are usually distributed using digital certificates, organizations often use a CA to manage this process. Technically, using a CA isn't required, as server applications can usually generate self-signed certificates without a CA. However, you can't easily use self-signed certificates to authenticate the identity of internal resources or devices outside of your organization. Self-signed certificates are recommended only for test or lab scenarios, as they are difficult to manage.

CRLs and OCSP

Occasionally certificates are issued in error and need to be invalidated, or they need to be invalidated for some other reason. This

Figure 2: Data integrity process

process is called certificate revocation. Each CA has a CRL that contains information about previously issued certificates that have yet to expire but are no longer valid.

The primary drawback of CRLs is that a large CA might need to revoke many certificates. Consequently, the CRL can grow quite large. When checking the status of a certificate, client OSs must retrieve the CRL in its entirety, which becomes bandwidth intensive. A delta CRL—a CRL that lists only the certificates revoked since the last complete (or base) CRL was issued—can help ease the problem. However, it doesn't provide the ideal solution because it, too, must be retrieved in its entirety.

OCSP is an HTTP protocol that uses minimal bandwidth to perform certificate status checks, as opposed to the clients downloading a CRL. OCSP determines certificate status by requesting information about a single certificate, so the volume of data returned to the client doesn't increase if the number of revoked certificates increases. Starting in Windows Server 2008 and Windows Vista, OCSP is enabled by default in Microsoft Internet Explorer (IE). The issuing certificate server must also support OCSP and configure certificates appropriately.

Chain of Trust

At some point, it becomes impractical for one CA to validate and issue certificates to every entity that requires one. Therefore, root CAs can grant subordinate CAs the right to issue certificates. This system creates a root/subordinate hierarchy.

The private key of a root CA certificate is used to sign the certificate of subordinate CAs. As long as a subordinate CA certificate is signed by the root CA certificate, certificates issued by the subordinate CA are valid within the hierarchy.

In the example of a web browser, root CA certificates are shipped with the client OS and provide a direct line of trust to public CAs, such as VeriSign and Thawte. If the CA that issued a certificate isn't directly trusted, the certificate chain must include a CA that's directly trusted.

Here's how the validation process works: The client OS checks the certificate's Issuer field to see which CA issued the certificate. Using the public key of the issuer's subordinate or root CA certificate, the client OS decrypts the digital signature of the certificate to be validated in order to read the signature's hash. The client OS then generates a second hash for the certificate to be validated and compares it to the hash from the decrypted signature. If both match, the certificate is considered valid.

The Big Picture

Let's take a look at how all the pieces fit into a PKI solution. SSL encryption is commonly used by websites and web browsers to verify the authenticity of a web server and encrypt data in transit over the public Internet. Transport Layer Security (TLS) is an advanced version of SSL (SSL 3.0 to be precise) commonly used for secure Internet transactions.

When a browser initiates communication, the web server and client OS first negotiate algorithm support. The server defaults to using the strongest standards that both the client OS and server support. The server then identifies itself by sending its public key in the form of a digital certificate. The client OS determines whether it trusts that certificate by checking the installed root CA certificates, checking the certificate's dates of validity, and making sure the certificate hasn't been revoked. Modern OSs, such Windows Vista and later, can also perform validation over the Internet using OCSP.

After validating the server's identity, the client OS creates a symmetric encryption key by generating a random number and encrypts it with the server's public key. The client OS then sends the encrypted key (the encrypted random number) to the server, which the server decrypts with its own private key. The new symmetric encryption key can then be used by the client OS and server to encrypt and decrypt message data.

The process of validating identities and exchanging a symmetric encryption key is known as a handshake. Once completed, encrypted message data is sent between the two parties.

Planning a PKI Solution

Now that you know how encryption, digital signatures, and digital certificates work, you can start planning how you want to secure your sensitive data. Start by deciding what you're trying to achieve: encryption, authentication, or both. Setting up and running your own PKI is no easy task (and there are associated ongoing management costs), so do research and determine whether PKI is required. Systems in which IPsec or domain isolation is applied often don't require a PKI. You should also consider possible future applications for PKI and make sure the solution you deploy is scalable. Finally, always follow best practices when deploying a PKI solution.

InstantDoc ID 129847

Russell Smith
(rms45@rsitc.com) is an independent IT consultant specializing in systems management and security, and author of *Least Privilege Security for Windows 7, Vista, and XP* (Packt).

Auditing Administrators' Actions with Exchange 2010

Protect your environment by maintaining records of who did what, to what, and when

by Tony Redmond

No one likes to think that someone else is checking up on his or her work, but it's an unfortunate fact of modern corporate life that actions often need to be audited and justified. For this reason, Microsoft Exchange Server 2010 introduced administrator auditing, which companies can use to audit the operations that administrators perform within an Exchange organization.

Apart from providing definitive proof about what account was used to add a mailbox, change a connector's properties, set up a new email domain, or perform another Exchange operation, maintaining an audit log can help satisfy legislative requirements by demonstrating that strict controls are imposed on the work performed by Exchange administrators. Some administrators won't welcome this increased oversight, viewing it as yet another example of big brother looking over their shoulder as they struggle to keep the email system up and running. Others will consider this increased oversight as part of modern life, much in the same way that people accept they're under the eyes of video surveillance wherever they go.

The Admin Audit Log agent—one of the standard cmdlet extension agents shipped with Exchange 2010—monitors administrative operations on Exchange 2010 servers, no matter what administrative interface is used. This is possible because the Exchange Management Console (EMC) and Exchange Control Panel (ECP) are built on top of the set of cmdlets exposed through the Exchange Management Shell (EMS), which means the execution of all business logic in Exchange 2010 flows through a common path. No indication is given in any administrative interface that auditing is in place, so administrators might be unaware that the details of their actions are being recorded.

Using the administrator auditing feature in Exchange 2010 isn't too difficult. I'll show you how to enable and configure administrator auditing and search the data that Exchange gathers about administrative actions. I'll also show you how to enable and configure a new mailbox auditing feature introduced in Exchange 2010 SP1. With this feature, you can discover when administrators and delegates log on to mailboxes and what actions they took.

Enabling Administrator Audit Logging

Administrator auditing consists of two components: the Admin Audit Log agent, which monitors administrator actions for auditing, and administrator audit logging, which writes the audit data to an audit mailbox. The agent is enabled by default, whereas the logging is disabled by default. Both the agent and the logging must be enabled for administrator auditing to occur.

To enable administrator audit logging, you need to use the Set-AdminAuditLogConfig cmdlet, which controls how the logging functions across the organization. In EMS, run the command

```
Set-AdminAuditLogConfig -AdminAuditLogEnabled $True
```

This new audit setting has to replicate across the organization before it's effective on all servers, so it might take an hour or so before you can be sure that all administrators' actions are being logged. However, logging will begin much sooner on the servers in the Active Directory (AD) site in which the command was run because the updated configuration will be available sooner to those servers. If you later

Table 1: Data Captured and Logged in Audit Entries

Property	What the Property Contains
RunDate	Date and time when the cmdlet was executed in Coordinated Universal Time (UTC) format
Caller	The user account that ran the cmdlet
CmdletName	The name of the cmdlet that was executed
CmdletParameters	The parameters and values specified for the cmdlet
ObjectModified	The object that the cmdlet was used to access (e.g., a mailbox)
ModifiedProperties	The properties that were modified by the cmdlet
Succeeded	True or False to indicate whether the cmdlet succeeded
Error	Details of any error message that was generated

want to disable administrator auditing, you'd run the Set-AdminAuditLogConfig command again, except this time you'd set the -AdminAuditLogEnabled parameter to *$False*.

Setting Up the Audit Mailbox

In the release to manufacturing (RTM) version of Exchange 2010, you have to create and configure a standard mailbox to act as the repository. You configure it by setting the Set-AdminAuditLogConfig cmdlet's -AdminAuditLogMailbox parameter to the mailbox's SMTP address. The address must be valid and belong to an authoritative domain in the organization. So, for example, the command might look like

```
Set-AdminAuditLogConfig
  -AdminAuditLogMailbox
  'AuditMailbox@contoso.com'
```

(Although this command wraps here, you'd enter it all on one line in EMS. The same holds true for the other commands that wrap.)

In Exchange 2010 SP1, you don't need to create and configure an audit mailbox. Instead, Exchange 2010 SP1 automatically creates the AdminAuditLogs folder in the Microsoft Exchange arbitration mailbox and stores the audit data in that folder. This arbitration mailbox is a more secure location for the audit data. Administrators can't grant themselves access, log on, and remove any audit entries that they don't want others to see, as they could with the standard mailbox. The arbitration mailbox uses a disabled account, so it takes more work to log on to it—and that work will leave some traces, revealing that an administrator might be up to no good.

No matter whether you're running Exchange 2010 SP1 or Exchange 2010 RTM, only one audit mailbox is used for an organization. This can pose some problems in widely distributed organizations; actions performed in one part of the network might have difficulty being registered in the audit mailbox. Even in highly centralized environments, it's still possible to see errors caused by the unavailability of the database that hosts the audit mailbox. During the period when the database can't be accessed, Exchange won't be able to capture audit entries. Exchange writes event 5000 (whose source is listed as MSExchange Management Application) into the application event log each time it's unable to log an audit entry. Administrator auditing will resume when the database becomes available, but any actions that occur when the mailbox is unavailable aren't captured.

Fine-Tuning the Audit Configuration

Once administrator auditing is running, the Admin Audit Log agent evaluates cmdlets as they're run against an audit configuration to decide whether the use of the cmdlet needs to be audited. By default, the agent captures information about the execution of every cmdlet that creates or amends data. It ignores the execution of cmdlets beginning with Get, Search, and Test to avoid cluttering up the audit log with entries for cmdlets that simply read or retrieve information or that test Exchange components.

If a cmdlet needs to be audited, the Admin Audit Log agent creates an entry containing details about the cmdlet's execution in the Inbox of the audit mailbox. Table 1 lists the default data that's captured and logged. If a cmdlet performs an action against several objects, the agent creates a separate audit entry for each object. For example, if an administrator uses the Set-Mailbox cmdlet to set new storage quotas for several mailboxes, the agent creates a separate entry for each mailbox when that database is updated with the new storage quota.

You can fine-tune the audit configuration to control exactly what information is captured. To view the current audit configuration, you use the Get-AdminAuditLog Config cmdlet. For example, the command

```
Get-AdminAuditLogConfig | Format-List
```

provides output like that in Figure 1. In this output, note the value of *{*}* for both AdminAuditLogCmdlets and AdminAuditLogParameters. These values tell Exchange to audit every cmdlet (excluding the exceptions noted previously) and every parameter in those cmdlets.

If you want to audit a specific set of cmdlets (i.e., actions), you can use Set-Admin AuditLogConfig. You specify which actions to audit with its -AdminAuditLogCmdlets parameter. For example, the command

```
Set-AdminAuditLogConfig
  -AdminAuditLogCmdlets 'New-Mailbox,
  New-DistributionGroup,
  New-MailboxDatabase, *Transport*'
```

```
AdminAuditLogEnabled     : True
TestCmdletLoggingEnabled : False
AdminAuditLogCmdlets     : {*}
AdminAuditLogParameters  : {*}
AdminAuditLogAgeLimit    : 90.00:00:00
AdminDisplayName         :
ExchangeVersion          : 0.10 (14.0.100.0)
Name                     : Admin Audit Log Settings
DistinguishedName        : CN=Admin Audit Log Settings,CN=Global Settings,
                           CN=contoso,CN=Microsoft Exchange,CN=Services,
                           CN=Configuration,DC=contoso,DC=com
Identity                 : Admin Audit Log Settings
```

Figure 1: Retrieving the current configuration for administrator audit logging

tells Exchange to audit the creation of new mailboxes, distribution groups, and mailbox databases. Plus, it tells Exchange to audit any action taken to manage the Microsoft Exchange Transport service (i.e., the use of any cmdlet whose name contains *Transport*).

If you want to capture only certain details about the new mailboxes created by administrators, you can use the Set-AdminAuditLogConfig cmdlet's -AdminAuditLogParameters parameter. For example, the command

```
Set-AdminAuditLogConfig
  -AdminAuditLogCmdlets 'New-Mailbox'
  -AdminAuditLogParameters 'Name,
  DisplayName, Custom*
```

captures only the name, display name, and values set for any of the 15 custom attributes (i.e., attributes whose names begin with *Custom*, such as Custom Attribute1) of the new mailboxes created by administrators.

You can write your own entries in the audit mailbox. For example, if you want to document a script being run or note a particular administrative operation you performed to solve a problem, you can use the Write-AdminAuditLog cmdlet in a command such as

```
Write-AdminAuditLog -Comment
  'Server acting up; cleared by
  increasing HeapSize to 30000'
```

You can insert up to 500 characters of text into the comment parameter, which is captured in the CmdletParameters property of the audit entry. If you use Write-AdminAuditLog, it's a good idea to write information into the custom audit entries that can be related back to other documentation, such as the reference number for a support ticket.

The audit configuration applies to administrative activity across the entire organization. All audit data goes into one mailbox, so it's easy to overload this mailbox if you audit an extensive set of cmdlets and parameters. You have to arrive at a balance between capturing the required data but not so much that it's difficult to find an instance when necessary. Some trial and error will likely be necessary.

If you're using Exchange 2010 SP1, you can also use an aging mechanism to control the amount of data in the audit mailbox. By default, audit entries are held for 90 days. The Managed Folder Assistant removes audit entries after their retention period expires. If you want to change the retention period, you can update it with the Set-AdminAuditLogConfig cmdlet's -AdminAuditLogAgeLimit parameter. For example, the command

```
Set-AdminAuditLogConfig
  -AdminAuditLogAgeLimit 182.00:00:00
```

sets the audit log retention period to 182 days (approximately six months).

The aging mechanism was introduced in SP1, so you won't have this option if you're running Exchange 2010 RTM. In that version, all of the audit data remains in the audit mailbox until you remove it.

Searching the Audit Data

Exchange 2010 RTM doesn't provide any out-of-the-box tools to search the audit logs and analyze administrators' activities. With this version, you have to open the audit mailbox and peruse the audit records to discover what has been captured.

Exchange 2010 SP1 addresses the lack of search tools two ways:

- It provides the new Search-AdminAuditLog cmdlet, which lets you search and analyze the audit logs in EMS. This cmdlet doesn't work against Exchange 2010 RTM audit entries because they're kept in a location unknown to the cmdlet.
- It provides a set of canned administrative and mailbox audit reports in ECP. These reports cover common reporting needs. These reports don't include any audit data collected in Exchange 2010 RTM's audit mailbox. This shouldn't be a problem in practice, though. You can delete the original audit mailbox after you've deployed Exchange 2010 SP1 throughout the organization.

Using Search-AdminAuditLog

With the Search-AdminAuditLog cmdlet, searching the audit logs is relatively painless. Here are a few examples of how you can discover what administrators are doing.

Search for actions performed by one or more administrators. Suppose you want to know the kind of operations being performed by certain administrators. You can identify the administrators by their aliases, email addresses, display names, or distinguished names (DNs), separated with commas. For example, the command

```
Search-AdminAuditLog
  -UserIds Administrator, AJR |
  Format-Table RunDate, Caller,
  CmdletName -AutoSize
```

tells Exchange to search for the actions of everyone who performed an action when logged in under the alias Administrator or AJR. As the sample results in Figure 2 show, most of the administrative activity that's unearthed has to do with mailbox databases and database availability groups.

Search for the execution of specific cmdlets. Suppose you want to know who has recently mounted or dismounted mailbox databases. To locate the audit records, you specify the cmdlets that are used for these purposes, as in

```
Search-AdminAuditLog
  -Cmdlets Dismount-Database,
```

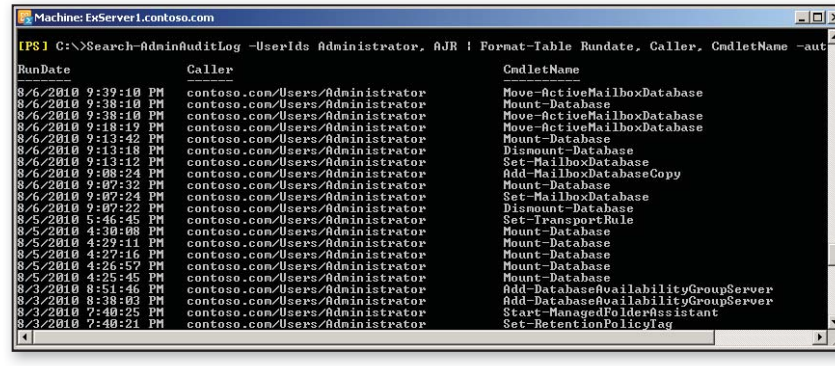


Figure 2: Searching for actions performed by specific administrators

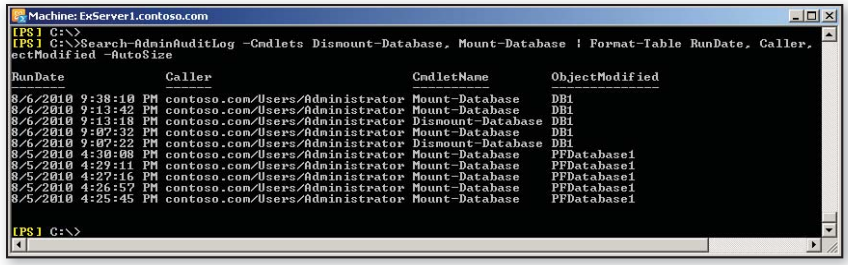


Figure 3: Searching for the execution of specific cmdlets

```
  Mount-Database | Format-Table RunDate,
  Caller, CmdletName, ObjectModified
  -AutoSize
```

The ObjectModified property tells you the name of the database in which the mount or dismount operation was performed. In the sample results in Figure 3, those databases were DB1 and PFDatabase1.

Search for audit records from a particular date range. Suppose you want to find out who was creating new mailboxes on a specific day. You can use a command such as

```
Search-AdminAuditLog
  -StartDate '08/13/2010 00:00'
  -EndDate '08/13/2010 23:59'
  -Cmdlets New-Mailbox |
  Format-Table RunDate, Caller,
  ObjectModified, Succeeded -Autosize
```

In the output set, note the Succeeded property, which specifies whether the cmdlet was successful. Some attempts to run the New-Mailbox cmdlet might fail, which is the case in the sample results in Figure 4. An attempt to create the *Hicks, Cassie* mailbox was unsuccessful for some reason.

One quirk with the Search-AdminAuditLog cmdlet is that it doesn't return the comments inserted into the audit log with the Write-AdminAuditLog cmdlet. As you'll recall, the comments store information that administrators want to add to the audit log, so it's important to be able to access that data. The data is held in the CmdletParameters property of the audit entry, but if you include this property in the output set, all you see is the string *Comment*. The data is in the audit log, but you need to extract it by directing the Search-AdminAuditLog cmdlet's output into an array, then looking at the appropriate element in that array. For example, the code

```
$AuditArray = Search-AdminAuditLog
  -StartDate '11/1/2010 00:00'
  -EndDate '11/1/2010 23:59'
$AuditArray[1].CmdletParameters
```

creates an array, then examines the CmdletParameters data in array element number 1.

Another quirk I noticed is that Exchange sometimes caches audit entries because they don't immediately show up in searches. I can't reproduce the problem all the time, but several times the audit entries didn't appear in searches until 5 to 10 minutes after they were created. The entries eventually show up, so data isn't being lost. You just have to be a little patient.

You also have to be patient if you attempt to execute a search when the database that hosts the audit mailbox is unavailable. To let you know, Exchange will give you the following message: *The attempt to search the administrator audit log failed. Please try again later.*

Using the Canned Reports

With SP1, ECP provides five reports on the Auditing Reports page, as Figure 5 shows. ECP uses cmdlets to obtain and process data from the administrative audit log, the mailbox audit log, and mailbox properties. For example, to generate the *litigation hold report*, ECP uses the Get-Mailbox, Search-AdminAuditLog, and Search-MailboxAuditLog cmdlets.

The *litigation hold report* lists the users who have been enabled for litigation hold (using EMC, ECP, or EMS) for a specified date range. This onscreen report tells you the account that enabled the hold and when the hold was applied.

The *non-owner mailbox access report* lists mailboxes that have been accessed or

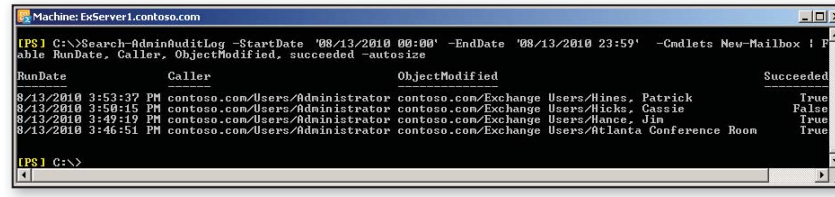


Figure 4: Searching for specific actions within a date range

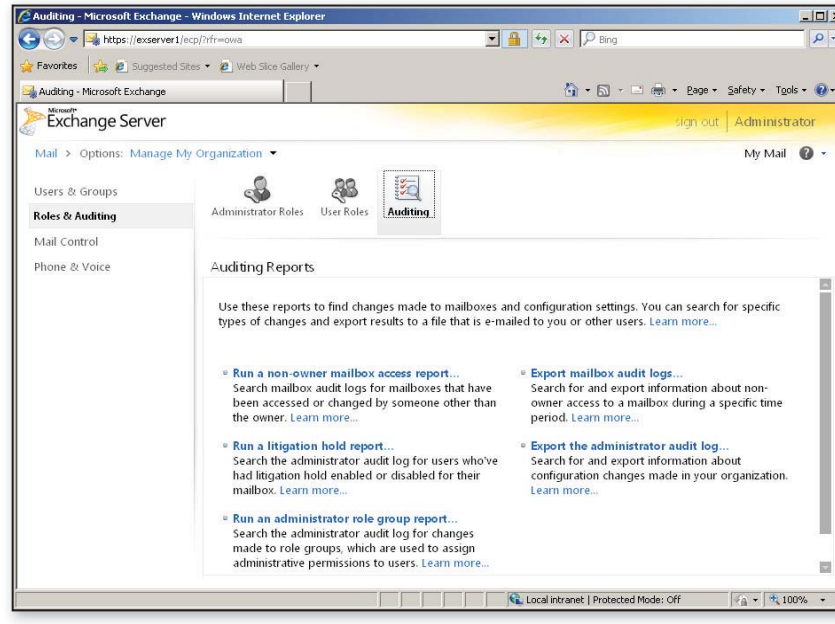


Figure 5: Using ECP's canned reports

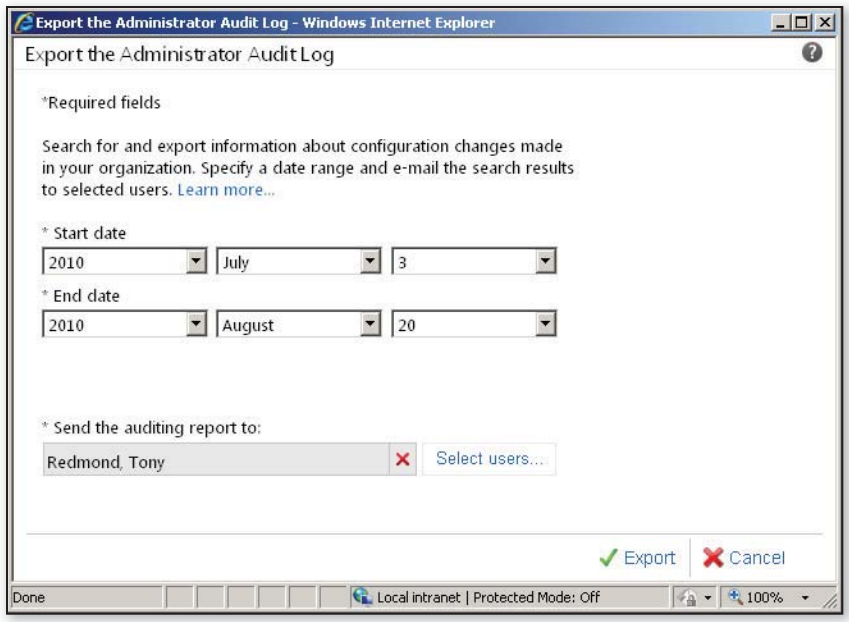


Figure 6: Exporting the administrator audit log

changed by a user other than the owner. If any events are found, they're listed along with information about what the non-owner did in the mailbox. For example, if a non-owner sent a message using SendAs permission, you'll can see the message's Subject line and whether the send operation succeeded. However, you can't see who the message was addressed to or what it contained. You'd have to conduct a separate mailbox search to retrieve this information. Although this report lets you check mailboxes that are being accessed by non-owners, it isn't a comprehensive audit report that will satisfy external litigators. It only points to activities that might need further investigation.

The *administrator role group report* lists the changes that have been made to role groups over a specified period. These actions grant permissions to users to perform the different administrative actions made available through membership of role groups. For example, membership in the Mailbox Import Export role group is required before you can import data from a PST into a mailbox, and membership in the Discovery Management role group is required before you can execute a multi-mailbox search. Again, this report only points to activities that might need further investigation, such as an account being granted a permission that it shouldn't possess.

If these three canned reports don't meet your needs, you can create custom reports. As previously demonstrated, you can easily explore the raw data with Search-MailboxAuditLog and other cmdlets.

The final two reports export the administrator audit log and the mailbox audit log so that you can peruse the data. These reports aren't displayed on screen. Instead, they're emailed to specified recipients. After you click either *Export the administrator audit log* or *Export mailbox audit logs* on ECP's Auditing Reports page, the basic steps in generating an export are:

1. Specify the period for which you want to export data (see Figure 6).
2. Specify the user or users who will receive the report.
3. Click the Export button.

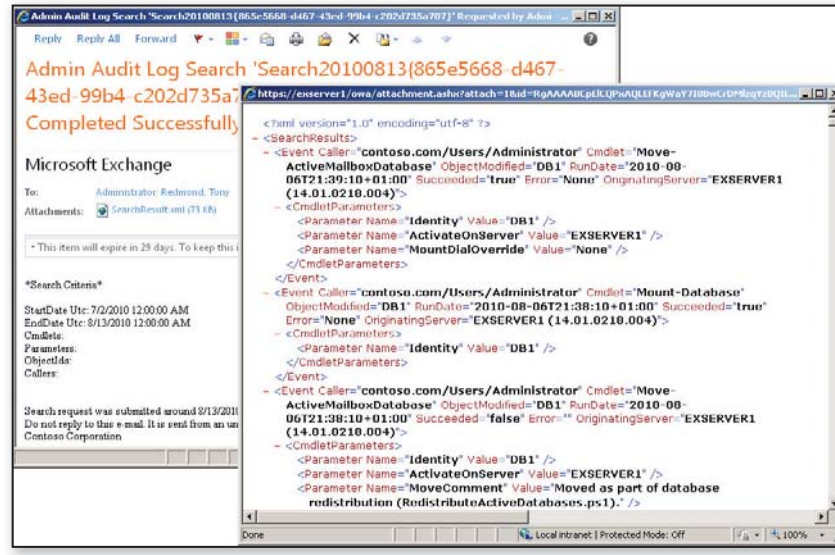


Figure 7: Opening the SearchResult.xml attachment

Unfortunately, ECP doesn't acknowledge the export request, but in the background Exchange starts searching for the required data. After the search results have been generated, Exchange sends the data to the recipients in the form of an XML attachment called SearchResult.xml. As you can see in the sample SearchResult.xml file in Figure 7, it contains the raw XML code. When you open the file in a browser or any other application that can open XML files, it reveals the actions taken by administrators.

You won't be able to access the attachment with Outlook Web App (OWA) unless you modify the OWA mailbox policy to permit XML files to be viewed. It's probably a bad idea to do this to the general-purpose OWA mailbox policy because it can create the potential for end users to unwittingly access XML content that might be malicious. It's a better idea to create a special OWA mailbox policy that permits access to XML attachments and assign that policy to administrators' mailboxes.

Enabling and Configuring Mailbox Auditing

Exchange 2010 SP1 introduces the ability to audit when owners, administrators, and delegates access mailboxes. Administrator auditing is enabled on an organizationwide basis, but mailbox auditing is enabled on an individual basis so that you don't have the overhead of gathering audit data for every mailbox in an organization. Instead, you can audit only those mailboxes that contain confidential information, such as executives'

```
Operation     OperationResult   LogonUserDisplayName  ItemSubject          LastAccessed
---------     ---------------   --------------------  -----------          ------------
SendOnBehalf  Succeeded         Executive Assistant   Budget Requests      11/14/2010 15:52:31
SendAs        Succeeded         Aha, Teresa           Note from Tony       11/15/2010 15:54:41
SoftDelete    Succeeded         Smith, John           Meeting with PR      11/15/2010 15:58:46
SendOnBehalf  Succeeded         Executive Assistant   Business standards   11/17/2010 16:05:09
```

Figure 8: Searching the mailbox audit data for actions performed by delegates

mailboxes or discovery mailboxes that hold the results of multi-mailbox searches.

An example of the kind of problem that mailbox auditing seeks to address is when rogue administrators give themselves full access to another user's mailbox, then log on to the mailbox to examine its contents. Although other versions of Exchange record an event indicating that the administrator logged on to the account, they don't tell you what the rogue administrator did afterward. But if the mailbox has been enabled for auditing in Exchange 2010 SP1, the audit will capture details of any auditable actions performed by the administrator. The same data is also captured for users who have been assigned delegate access to the mailbox by its owner.

Mailbox auditing is enabled through the Set-Mailbox cmdlet. For example, if you want to protect the CEO's mailbox, you could use a command such as

```
Set-Mailbox -Identity 'CEO Mailbox'
  -AuditOwner $Null
  -AuditDelegate Update, Move,
    MoveToDeletedItems, SoftDelete,
    HardDelete, SendAs, SendOnBehalf
  -AuditEnabled $True
```

In this command, setting the -AuditEnabled property to $True turns auditing on for the mailbox. The -AuditDelegate parameter tells Exchange to audit any action that updates content, moves items, deletes items, empties the Deleted Items folder, or sends messages from the mailbox if that action is performed by the delegate. In this context, a delegate is someone who logs on to the mailbox using SendAs, SendOnBehalf, or FullAccess permission. You can also audit administrators' access to a mailbox by specifying the -AuditAdmin parameter (which isn't shown here). Auditing can be enabled for mailbox owner access as well, but it isn't typically done because of the high number of audit items that result.

Mailbox audit data is stored in the Audits subfolder of the Recoverable Items folder in the user's mailbox. Mailbox audit items are kept for 90 days by default, but this setting is customizable up to 68 years.

Searching the Mailbox Audit Data

You have several methods you can choose from to search the mailbox audit data:

- ECP's canned report. The *Export mailbox audit logs* option in ECP's Auditing Reports page exports the mailbox audit data for perusal.
- Search-MailboxAuditLog. This cmdlet performs a synchronous search for one or more mailboxes and returns the results on screen.
- New-MailboxAuditLogSearch. This cmdlet searches across one or more mailboxes asynchronously in the background and emails the results.

Because I already covered how to use the ECP canned report, let's jump right to the Search-MailboxAuditLog cmdlet. An example of how to use this cmdlet is

```
Search-MailboxAuditLog
  -Identity 'CEO Mailbox' -ShowDetails
  -StartDate '11/14/2010 00:01'
  -EndDate '11/17/2010 23:59'
  -LogonType Delegate -ResultSize 100 |
  Format-Table Operation,
    OperationResult,
  LogonUserDisplayName, ItemSubject,
  LastAcccessed
```

This synchronous search looks for audit entries in the CEO's mailbox and reports any found that occurred through delegate access. Figure 8 shows sample results.

An example of how to use the New-MailboxAuditLogSearch cmdlet is

```
New-MailboxAuditLogSearch -Name
  'Unauthorized Delegate Access review'
  -LogonTypes Delegate
  -Mailboxes 'CEO Assistant', 'CEO',
  'Senior VP-Finance'
  -StartDate '1/1/2010'
  -EndDate '12/31/2010'
  -StatusMailRecipients
  'ComplianceAuditMailbox@contoso.com'
```

This background asynchronous search looks for audit entries in the three specified mailboxes and sends the output to an SMTP address, which doesn't necessarily have to be an Exchange mailbox.

Considerations to Keep in Mind

It'll take some time for companies to decide whether they want to implement administrator or mailbox auditing, what kind of actions they will audit, how long to keep the audit data, and how they will use that data. When you help your company make those decisions, you need to keep a couple of considerations in mind.

First, capturing audit data for administrator actions or mailbox access doesn't replace the need for careful recording of server and organization configuration changes. To help ensure the smooth operation of your Exchange organization, you still need to document changes when you perform activities such as:

- Testing and applying hot fixes and updates, including new service packs for Exchange
- Testing and applying Windows service packs
- Making major network updates (e.g., introducing a new DNS server)
- Installing new Windows and Exchange servers
- Installing new software on an Exchange server
- Updating transport configuration updates (e.g., adding a new connector, changing transport settings)

Second, remember that administrator auditing works only on Exchange 2010 servers. It won't work, for instance, if an administrator makes a change to a mailbox database or transport connector on an Exchange 2007 server in a mixed-mode organization. That issue will go away as servers are upgraded to Exchange 2010.

InstantDoc ID 129720

Tony Redmond
(12knocksinna@gmail.com) is a contributing editor for *Windows IT Pro*, and author of *Microsoft Exchange Server 2010 Inside Out* (Microsoft Press). His blog is available at thoughtsofanidlemind.wordpress.com.

Deploying FAST Search Server 2010 for SharePoint

This powerful add-in raises the bar for speedy and effective content searches

by Agnes Molnar

There's just no substitute for speed. SharePoint Server 2010 already offers enhanced and powerful search capabilities. But if you decide to deploy FAST Search Server 2010 for SharePoint on top of the native search functionality, you'll get a much richer and much more powerful experience. The following are the key benefits of FAST Search Server 2010 for SharePoint:

- a deep refinement panel that shows the amount of results in each refinement category
- ability to sort on any property
- document thumbnails and previews
- the Visual Best Bets search feature
- document and site promotion and demotion capability
- user context from user profiles that let you differentiate users and the way in which the results display to them
- a "similar search" feature
- extreme scale-out of up to more than 500 million documents
- easy administration and configuration, fully integrated into SharePoint 2010
- content processing pipeline
- entity extraction

Although the deployment process for FAST Search for SharePoint may seem to be easy and self-evident, you should learn a few tricks to make your job much easier. The following are the logical steps to deploy FAST Search Server 2010 for SharePoint:

1. Install FAST Search for SharePoint
2. Configure FAST Search for SharePoint
3. Deploy Search service applications (create FAST Query SSA and FAST Content SSA)
4. Deploy a FAST Search Center

Step 1: Installing FAST Search Server 2010 for SharePoint

FAST Search Server 2010 for SharePoint (aka FAST for SharePoint 2010—F4SP) can be installed on top of a SharePoint Server 2010 Enterprise farm. As a fully integrated component, FAST Search for SharePoint can also contain one or more servers from a FAST farm. The obligatory FAST admin server is responsible for running administrative services. Non-admin servers can also be added to the deployment to handle non-admin services, such as query matching, indexing, document processing, and so on. In a single-server environment, these two roles are handled by the same server; however, a multi-server deployment can contain one admin server and one or more non-admin servers. The following steps to install FAST Search for SharePoint are pretty straightforward:

- Create a domain user for FAST administration tasks. (For example, create DOMAIN\fastadmin). This user
  - must be a domain user
  - must be a member of the FASTSearchAdministrators group on the FAST admin server
  - must have sysadmin privileges on the SQL Server system

- Install Office Web Apps. (To get the installation files, see office .microsoft.com/en-us/web-apps.) Office Web Apps is required for some FAST Search for SharePoint features, such as document thumbnails.
- Install FAST Search Server 2010 for SharePoint prerequisites. Similar to SharePoint 2010, these prerequisites can be installed by the FAST Search for SharePoint installation wizard, or you can install these components manually. In either case, you must deploy the following prerequisites before you install FAST Search for SharePoint:
  - Application Server role, Web Server (IIS) role
  - Distributed transaction support
  - Windows Communication Foundation Activation Components
  - XPS Viewer
  - Microsoft .NET Framework 3.5 SP1
  - Hotfix for Microsoft Windows (KB 976394)
  - Windows PowerShell 2.0
  - Windows Identity Foundation (KB 974405)
  - Microsoft Primary Interoperability Assemblies 2005
  - Microsoft Visual C++ 2008 SP1 Redistributable Package (x64)
  - Microsoft Filter Pack 2.0

- Run the FAST Search Server 2010 for SharePoint installation wizard, and select the *Install FAST Search Server 2010 for SharePoint* option.

Step 2: Configuring FAST Search Server 2010 for SharePoint

After your installation is finished, you must configure your FAST Search for SharePoint environment. To do this, follow these steps.

Note: For a multi-server deployment, see the information that follows this procedure.

1. Click Start, type *Microsoft FAST* in the Start Search box, then click the *Microsoft FAST Search Server 2010 for SharePoint / FAST Search Server 2010 for SharePoint Configuration Wizard* link.
2. Select deployment types:
   - Single Server: a standalone installation, including both admin and non-admin components
   - Admin Server: in a multi-server deployment, the admin component to which the non-admins will connect
   - Non-admin Server: in a multi-server deployment, a non-admin component (you must deploy a FAST admin server before you deploy a non-admin component)
3. Enter the FAST username and password that you created.
4. Enter a certificate password.
5. Specify server settings:
   - FQDN of the FAST admin server (for example, f4sp .demo2010.local)
   - base port that will be used to calculate how to reserve the required ports for FAST Search for SharePoint (the default value is 13000)
   - database connection string: FQDN of the SQL Server system on which FAST Search databases will be created (for example, sql .demo2010.local)
   - name of the FAST Admin Database (for example, FASTSearchAdminDatabase)
6. Provide the click-through relevancy settings by selecting the SharePoint Server installation type: Standalone, Server Farm, or *Do not enable click-through relevancy*.
7. Follow these post-configuration steps:
   a. Verify whether your FAST admin user is a member of the FAST-SearchAdministrators group on the FAST admin server.
   b. Open the Microsoft FAST Search Server for SharePoint PowerShell command, and run the following command:

```
nctrl status
```

   c. Make sure that all services are running.
8. Restart the server.

In a multi-server deployment, you must create a deployment.xml file. This file describes the topology of the FAST Search architecture. The deployment.xml file should resemble the example file shown in Figure 1.

For more information about this procedure, see the Microsoft article "Configure a stand-alone deployment or a multiple server deployment (FAST Search Server 2010 for SharePoint)" (technet.microsoft .com/en-us/library/ff381240.aspx#BKMK_ ConfigureAMultipleServerDeployment).

Step 3: Deploying Search Service Applications

After you complete the configuration of FAST Search, you have to take additional steps to prepare your SharePoint 2010 environment for this added feature.

The logic of the preparation process is the same as the logic for deploying the out-of-the-box SharePoint Search itself. First, create the appropriate search service applications. In the case of FAST Search for SharePoint, the following search service applications are required:

- FAST Content Service, for crawling and feeding content for the FAST back end

```
<?xml version="1.0" encoding="utf-8" ?>
<deployment comment="3 node FAST Search farm configuration"
      xmlns="http://www.microsoft.com/enterprisesearch">
 <instanceid>FASTSearchMultiNodeDemo</instanceid>

 <connector-databaseconnectionstring />
 <host name="fastserver1.contoso.com">
  <admin />
  <indexing-dispatcher />
  <content-distributor />
  <webanalyzer server="true" link-processing="true"
     lookup-db="true" />
  <document-processor processes="2" />
 </host>
 <host name="fastserver2.contoso.com">
  <searchengine row="0" column="0" />
 </host>
 <host name="fastserver3.contoso.com">
  <searchengine row="1" column="0" />
  <query />
 </host>
 <searchcluster>
  <row id="0" index="primary" search="true" />
  <row id="1" index="none" search="true" />
 </searchcluster>
</deployment>
```

Figure 1: Sample code for Deployment.xml

THE TOP 10

Best Practices for Locking Down Corporate PCs

—By David Chernicoff

Control is always an issue for corporate IT. End users have a tendency to treat their office computers as their own property and not as a corporate resource. This means that end users will often try to install software on their own, download content that isn't business appropriate, and take actions that expose the computers to external threats. Beyond causing problems for IT, there is also the potential for business liability in the way that end users utilize an unrestricted computer. Ranging from regulatory compliance issues to simple misuse of corporate data, the potential liability of unfettered computer use can be significant.

1 We're migrating to Windows 7. What else should we consider?

You've decided to make a corporate-wide switch to the latest version of Windows. That makes this the perfect time to implement the system control policies that your business needs. End users should have the privilege level that they need to get their job done and there may be other issues that mandate your having better control of your endpoint computers. Implementing privilege management with the operating system upgrade is a natural fit. As you deploy the new operating system images or brand new systems you have an opportunity to simultaneously roll out the privilege management agent. End users are well known for finding workarounds that allow them to install non-standard applications such as instant messaging. Locking down everything can prevent this, but at a cost—usually productivity, because systems can become awkward to use and difficult to make handle the unexpected task. This is where a privilege management solution is extremely beneficial. Systems are less at risk without sacrificing user productivity or increasing support call volume, thereby offering a cost-effective approach to providing secure and productive desktop computing environments.

2 Who has access to what?

When was the last time you performed a serious assessment of access control and user rights within your network? It's time to find out who has control over what, where users and groups have administrator rights, and evaluate the group and user needs for elevated levels of control. Use this opportunity to determine exactly who's who in terms of administrative control of your corporate desktop. Is it more users than just the IT staff? Are there unknown administrators who exist inside or outside of your Active Directory infrastructure?

3 Dealing with compliance issues.

Many regulatory requirements deal directly with access control. Giving the wrong users access to regulated data can result in serious repercussions for your business, ranging from lost contracts to government-imposed fines. Having detailed control over your end user computers is a big step toward preventing these types of access control failures and problems. With the right privilege management application you're able to track changes to the subsystem (e.g., application installation and configuration changes), audit potentially suspicious or unapproved activity, and monitor the administrators who are responsible for enforcing desktop policy.

4 Watch out for automated updates.

Microsoft releases patches and hotfixes regularly. Not controlling how and when those fixes are deployed within your environment is a recipe for disaster. Controlling end user administrator rights is essential to controlling hotfixes. Simply stated, when end users don't have administrator rights, the desktop is less vulnerable to a variety of malware. Desktop lockdown compliments other security measures and provides an additional layer of defense against malware.

5 "One size fits all" doesn't work.

Granularity in privilege management is what will allow it to work for the most complex environment. Although some access control policies can be effective when utilized across the board, the best fit for

your business, and the most effective way to utilize privilege management, requires a much more granular level of control. You can use this level of granular control to formulate corporate policies for data and application access. You also can apply granular control across all types of automated policy management to allow a multidimensional approach to common access control issues, ranging from what applications can utilize which data to an allowable time of day for a user to be accessing information. Group Policy alone is incapable of the fine level of control necessary for most effective desktop utilization.

6 Automation makes detailed control practical.

It would be impractical for IT staff to explicitly design and configure the appropriate level of privilege for each user. With good automation tools, IT can apply appropriate levels of privilege to end users based on their ad hoc business needs, without direct intervention for each and every user. Automated policies, combined with privilege management features, allow IT to be more effective in maintaining data and information security.

7 Managing mobile users

Many organizations have users who rarely, if ever, are directly connected to the corporate network. This makes managing their user rights problematical. Their notebook is still a corporate asset and needs to be properly managed, but it might not be part of the corporate Active Directory (AD), or it might be connected to the main network so rarely as to make management via standard group policies ineffective. With the right privilege management tool, IT should be able to apply administrative standards to any computer for which they are responsible, even mobile users not in the AD. Offline or online, all policies should continue to be enforced with minimal impact on the console user.

8 Allowing applications to run properly.

There is always the concern that limiting user rights will prevent applications from running properly. Although Windows allows applications to run with a different user context and the applicable rights for that user, third-party tools are needed to provide more detailed control and to allow applications to run properly without requiring a change in user context. An effective privilege management tool allows you to design and enforce policies in a way that achieves your company's objectives without creating unnecessary restrictions on the end user. Look for privilege management features that provide application-level control and policy customization on the desktop. Many situations that formerly required complete lockdown can now be managed via policies without creating excessive limitations on the end user machine. By using this more granular control you reduce the risk associated with running applications that require elevated user rights.

9 Auditing and configuration control.

Keeping track of the privilege policies, compliance, and changes that are made to access rights and privileges is important for a number of reasons. Regulatory compliance, policy monitoring, and the effects of different operations within the computing environment are all important in keeping an effective and secure operation running. This can also be an incredibly difficult task for casually connected users. People who work away from the corporate network, or who are rarely connected, can have problems getting effective use of their systems if the only control IT is able to enforce is overly restrictive Group Policies. Using an effective privilege management tool means that end user capabilities on the system can be more clearly defined and end users can be given the access they need to do their job without granting overly permissive user rights.

10 Examining the effect of privilege-level management.

Once you understand what you need your privilege management product to do, it shouldn't be a difficult process to get it up and running in your environment. The selected product should provide capabilities that allow IT to enhance already implemented policies and adapt to situations on the fly that are critical to effective privilege management. Logging user activities, generating informative reports on how client PCs are being used and where user rights are not properly contained, and integration with Microsoft System Center Configuration manager are important features to look for in a privilege management solution. The privilege management product should be able to go far beyond the limited capabilities of GPO add-ins, especially in regards to mobile and casually connected users. Implementing an effective privilege management solution should be seen as a clear win for IT.

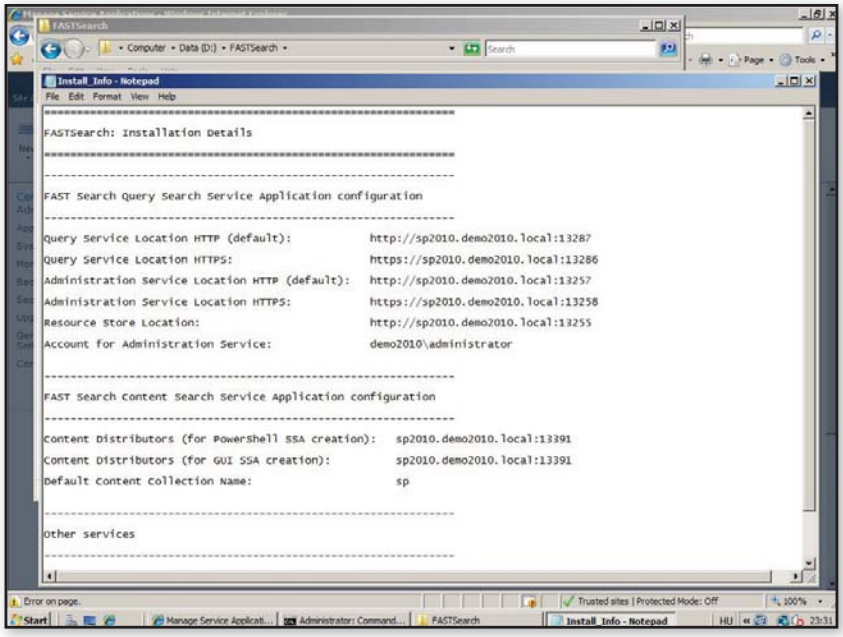


Figure 2: FAST Search installation details

- FAST Query Service, for serving the queries and crawling the People content source

Note: The FAST Query Service routes the People search to the SharePoint 2010 Search engine, and routes all other queries to the FAST Search engine.

To deploy these service applications, you have to provide some URLs and port numbers, which are based on the base port that you configured previously. You can find the required information in the install_info.txt file in the FASTSearch folder. Another important file is contentdistributor .cfg in the FASTSearch\etc folder. This file contains the exact location of the content distributors, shown in Figure 2.

To create a FAST content service application, follow these steps:

1. Navigate to the Central Administration site of your SharePoint 2010 farm.
2. In the Application Management section, click Manage Service Applications.
3. Click the Service Applications tab, click New, then click Search Service Application (see Figure 3).
4. Type a descriptive name. For example, type *FAST Content Service App*.
5. For the service application type, select FAST Search Connector.
6. In the Application Pool list, select an application pool, or create a new application pool.
7. Enter the location of the content distributors.

Note: The Install_info .txt file contains the URLs for the content distributors.

8. Open the install_info.txt and the contentdistributor.cfg files to locate the URLs and port numbers that are required during the installation.
9. Enter the name of the content collection.

Note: Enter the default name of "sp" if you didn't configure the name of the content collection during the installation.

10. To save your changes, click OK.

After you finish configuring your SharePoint 2010 farm, the farm is connected to the FAST Search content, and you're able to crawl the content immediately (as shown in Figure 4.

The next step is to create the FAST Query Service application to enable running queries against the crawled and indexed content. To create this application, follow these steps:

1. Navigate to the Central Administration site of your SharePoint 2010 farm.
2. In the Application Management section, click Manage Service Applications.
3. Click the Service Applications tab, click New, then click Search Service Application.
4. Type a descriptive name. For example, type *FAST Content Service App*.
5. For the service application type, select FAST Search Connector.
6. In the Application Pool list, select the appropriate application pool for both the Search Admin Web Service and the Search Query and Site Settings Web Service, or create a new application pool.
7. Enter the location of the following services:
   - Query Service
   - Administration Service
   - Resource Store

   Note: You can find these URLs in the install_info.txt file.
8. Enter the FAST admin account that you created previously. For example, enter DOMAIN\FASTadmin.
9. To save your changes, click OK.

Now that you've integrated FAST with SharePoint 2010, you're almost ready to start using your FAST Search environment. But first, you have to create and import the certificate that will apply to the communication between SharePoint 2010 and FAST Search. To do this, follow these steps:

1. Run the SharePoint 2010 Management Shell as an administrator.
2. Run the following PowerShell commands:

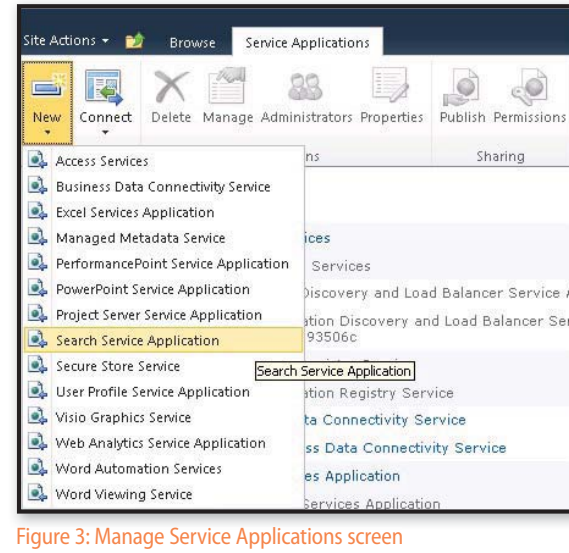


Figure 3: Manage Service Applications screen

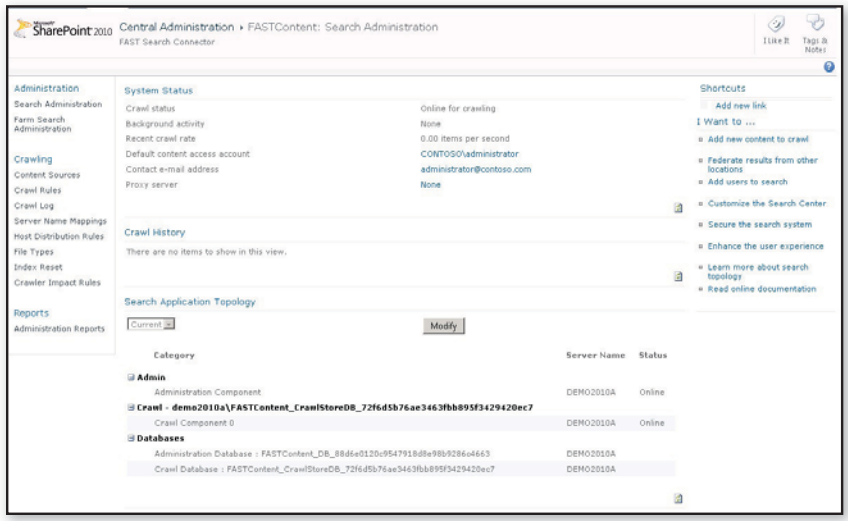


Figure 4: Central Admin FAST Search Connector crawl screen

```
$stsCert = (Get-
  SPSecurityTokenServiceConfig)
  .LocalLoginProvider.SigningCertificate
$stsCert.Export("cert") | Set-Content
  -encoding byte MOSS_STS.cer
```

3. Import the certificate created in step 2 into the Trusted People certificate store on your FAST Search server (as shown in Figure 5).

With the communications certificate in place, FAST Search Server 2010 for SharePoint is deployed successfully and is almost ready for use.

Step 4: Deploying FAST Search Center

Now that you've installed and deployed the FAST Search Server architecture on SharePoint 2010, the following preparation steps remain before you can use the full functionality of FAST Search for SharePoint:

- crawl and index the content
- create the required scopes
- deploy a FAST Search Center

Usually, you can apply crawl settings at the FAST Content Site Service Account (SSA). The Crawl service application is responsible for crawling all content, including SharePoint, file shares, Exchange public folders, and custom content sources. To define the content sources that are required to be crawled, follow these steps:

1. Navigate to the Central Administration site of your SharePoint 2010 farm.
2. In the Application Management section, click Manage Service Applications, and open your FAST Content SSA.
3. On the Quick Launch menu under Crawling, click Content Sources.
4. In the Content Sources list, select the appropriate content sources, or create new sources.

Note: Be careful not to select People as a content source because the People search is performed by the SharePoint search engine, not by FAST. Therefore, the People selection should be made on the FAST Query SSA instead of on the FAST Content SSA.

5. Right-click Content Source, and then click Start Full or Incremental Crawling.

Note: This is the same method to start these operations as in SharePoint 2010 Search.

After the contents are crawled, deploy the content search scopes. Because the search scopes are part of the Query process, they can be found in the FAST Query SSA. To deploy the search scopes, follow these steps:

1. Navigate to the Central Administration site of your SharePoint 2010 farm.
2. In the Application Management section, click Manage Service Applications, and open your FAST Query SSA.
3. On the Quick Launch menu under Queries and Results, click Scopes to locate the scopes that are defined for your FAST Search.

Note: As in SharePoint 2010 Search, two scopes are defined here by default: All Items and People. However, you might have to configure additional scopes.

After your scopes are configured correctly and ready to use, it's finally time to search! To search the content crawled by FAST in SharePoint 2010, you must create a FAST Search Center. To do this, follow these steps:

1. Navigate to the collection site on which you want to create the FAST Search Center.
2. On the Site Actions menu, click Create.
3. In the list of site templates, click FAST Search Center.
4. Complete the template, and save the new Search Center.

And that's it. Figure 6 shows a completed Search Center. If your configuration has been successful, you can immediately enjoy the functionalities of FAST Search Server 2010 for SharePoint!

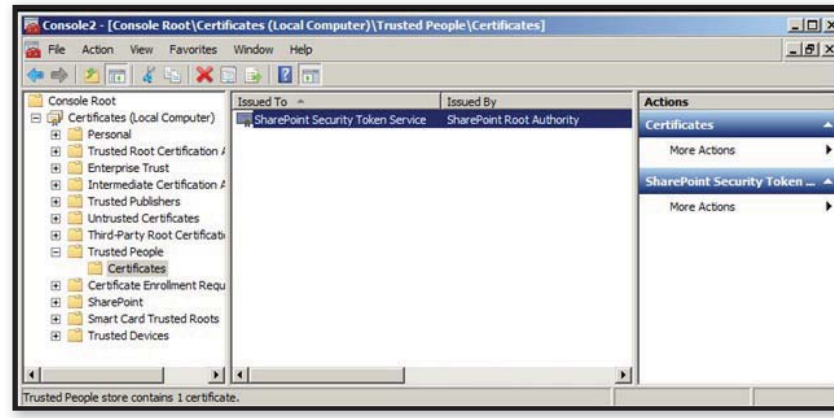


Figure 5: Trusted People-Certificates screen

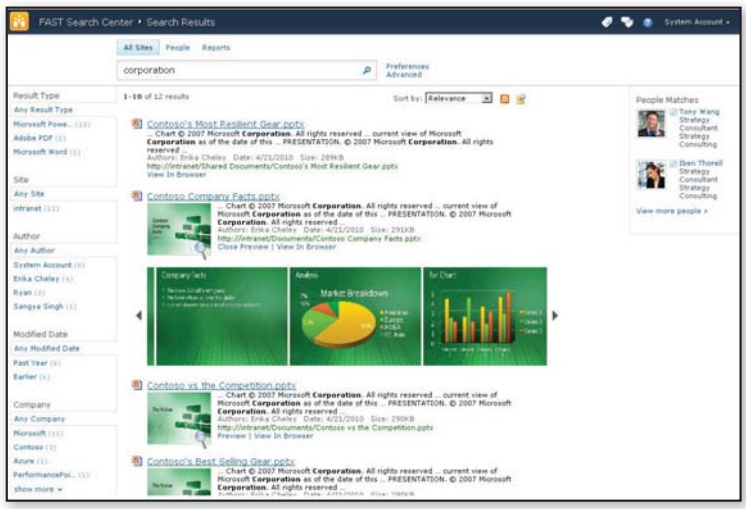


Figure 6: FAST Search Center FAST Search results page

Troubleshooting FAST Search Deployment

If you experience any errors during the FAST Search Server 2010 for SharePoint deployment, the following useful tricks can help you debug and troubleshoot the installation:

- Manually push some content to the FAST content collection. You can verify whether you're able to do this by following these steps:
  - Create a simple document on your local computer. For example, create a document named FASTtest.txt. Type some sample content in the file. For example, type *Hello World! This is my test document*.
  - Run the Microsoft FAST Search Server 2010 for SharePoint shell.
  - Run the following command:

```
docpush -c <collection name>
  "<fullpath to your file>"
```

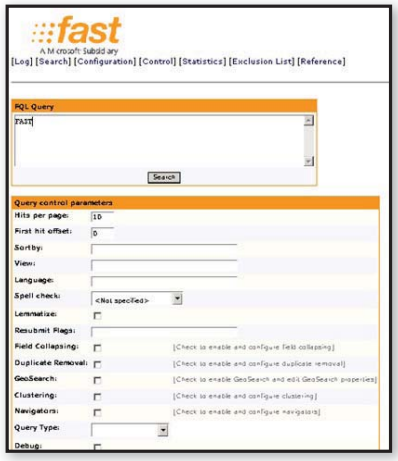


Figure 7: FQL test page

For example, run the following command:

```
docpush –c sp "C:\FAST_test.txt"
```

For full docpush reference information, see the Microsoft article, "docpush reference" (technet.microsoft.com/en-us/library/ee943508.aspx).

After this command runs successfully, the document is pushed into the FAST content collection, and the document can then be queried. Of course, you can add more documents to the content collection before you test the search functionality.

- Run an FQL test on the content collection. To do this, follow these steps:

  a. Open a browser window on your FAST server, and visit the FAST Query Language (FQL) test page at http://localhost:[base_port+280]. For example, if you use the default base port of 13000, the URL for the FQL test page is http://localhost:13280/.

  b. Search on a word that's contained in the test document that you uploaded (C:\FAST_test.txt). For example, search on "world" or "test." The result set should contain your test document.

  Note: You can also set other parameters on the FQL testing page, such as language, debug information, and so on.

What does an FQL test tell you after you receive an error message from the FAST Search Center? A failed test query tells you that something is wrong in your FAST configuration. A successful test query tells you that some kind of communication problem exists between FAST and SharePoint.

- Use these tips to troubleshoot the following error scenarios:
  - *The search request was unable to connect to the Search Service*: This message indicates that SharePoint cannot connect to the FAST Search engine. This may occur for several reasons. In most cases, some URL or port settings are wrong on a FAST service application. This problem may also occur because the FAST Query service application is not associated with the current Web application.
  - *Unable to display this Web part*: This message indicates that something is probably misconfigured in FAST Search Server for SharePoint 2010. Verify the URL and port numbers again.
  - If Microsoft Word and Microsoft PowerPoint thumbnails are not displayed in the result set, a problem exists in your Office Web Apps installation. Either the program is not installed correctly or it's not enabled on your site.

    Note: When the FAST Search service runs its initial crawl, it can take a long time to generate and display the document thumbnails and previews.

Looking Ahead

Unless you experience any deployment errors, you should now be all set to put FAST Search Server 2010 to work. In a future article, I'll provide more detail about F4SP functionality, additional deployment troubleshooting help for FAST Search, and some best practices for this powerful search engine.

InstantDoc ID 129827

Agnes Molnar
(aghy@aghy.hu) is an MVP, MCT, and MCPS. She has been working with Microsoft technologies and SharePoint since 2001. After MOSS 2007's release, she founded a SharePoint consultant company in Hungary, Central Europe. Agnes's main focus is on enterprise search, information architecture, and knowledge management and governance. She's a co-author of the book *Real World SharePoint 2010*.

“THE CONVERSATION BEGINS HERE”

UNIFIED COMMUNICATIONS CONNECTIONS

Microsoft® Exchange CONNECTIONS

WINDOWS CONNECTIONS

SharePoint CONNECTIONS

Microsoft® Visual Studio® CONNECTIONS

Microsoft® ASP.net CONNECTIONS

Microsoft® Silverlight® CONNECTIONS

SQL Server CONNECTIONS

QUESTIONS ANSWERED • STRATEGY DEFINED • RELATIONSHIPS BUILT

OCT 31-NOV 3, 2011
LAS VEGAS, NV
MANDALAY BAY RESORT & CASINO

Make **CONNECTIONS** the **CONFERENCE** you bring your whole team to this year!

Only Microsoft and industry experts speak at WinConnections!

- Train with 100+ Microsoft & Industry Experts at over 240 deep dive sessions.
- Attend cutting edge keynotes & keep your competitive edge.
- Network with Microsoft, industry experts, and colleagues.
- Attend the co-located event sessions at no extra charge.

MARK MINASI
MINASI RESEARCH AND DEVELOPMENT

STEVE FOX
MICROSOFT

SCOTT GUTHRIE
MICROSOFT

JIM MCBEE
ITHICOS SOLUTIONS

DON JONES
CONCENTRATED TECHNOLOGY

RHONDA LAYFIELD
DEPLOYMENTDR.COM

CHECK WEB SITE FOR DESCRIPTIONS OF SESSIONS AND WORKSHOPS

www.WinConnections.com • 800.505.1201 • 203.400.6121 • Register Today!

Microsoft · SharePointPro CONNECTIONS · SQL Server MAGAZINE · Windows IT Pro · TECH Conferences Inc. PENTON MEDIA

Exchange Server's Client Access: Server Administration

Management, monitoring, and troubleshooting

by Ken St. Cyr

It's 4:55 P.M. on Friday and just as you pack up your stuff and get ready to leave the office, the phone rings. You answer the call and find out that users are having trouble connecting to their mailboxes through Outlook Anywhere. What do you do? And how do you prevent this problem from recurring? In this last article of my five-part series on the Microsoft Exchange Server Client Access role, I discuss Client Access server administration, including what you need to monitor on a regular basis to help ensure that your Client Access servers are operating at optimal health and what to do when things go wrong. (For earlier articles in the series, see the Learning Path.)

Your Client Access servers make up only a slice of your Exchange Server 2010 infrastructure. Other Exchange server roles require an equal or greater amount of attention on a regular basis, and each role has its own focus for administration. Because the primary responsibility of the Client Access role is to facilitate connectivity for your messaging clients, it should come as no surprise that your focus in administering this role is to ensure that your clients can successfully connect to your Exchange organization and access their mail. The administration of the Client Access role can be summed up in three basic tasks:

1. Managing Client Access role settings
2. Monitoring servers' performance and diagnostics
3. Troubleshooting problems that arise

Managing the Role Settings

Even after your Client Access servers are up and running, you'll likely need to adjust their configuration periodically. The Client Access role has multiple settings that you can manage; the most common ones are exposed through Exchange Management Console (EMC). For less common settings, you need to use Exchange Management Shell (EMS), either remotely or from an Exchange server.

You can remotely manage your Client Access servers in one of two ways. The first method is to install Exchange Management Tools on your workstation. Installing these tools gives you the same functionality that

Figure 1: Installing Exchange Management Tools

Table 1: Important Hardware Performance Counters

Counter	Notes
Processor (_Total)\% Processor Time	Percentage of time the processor is being used; on average, this number should be under 75 percent. If processor utilization exceeds this number, your server is considered overutilized. In this case, you should look at the CPU utilization for the running processes and determine whether the overutilization is because of a large user load. If so, you should consider adding servers to your Client Access array.
Processor (_Total)\% User Time	Reports the time the processor is being used for non-kernel (also known as "user-mode") activities; should be under 75 percent. If this counter exceeds 75 percent, an application running on the server is probably causing the overutilization. In this case, you should determine which process is at fault. If it's a non-Exchange component, you should consider removing the process or moving it to another server. If it's an Exchange component, you should add servers to your Client Access array.
Processor (_Total)\% Privileged Time	Percentage of time the processor is being used for kernel mode activity; should be under 75 percent. If this counter exceeds 75 percent, an OS component is probably causing the overutilization. Before deciding to add servers to the Client Access array, you should make sure that the latest OS updates are installed and check with the server manufacturer to ensure that the server has the latest firmware and drivers. Sometimes (but not always) overutilization in the kernel can be attributed to driver-level bugs or bugs in the OS.
System\Processor Queue Length (all instances)	Number of threads waiting to be scheduled for execution; should be fewer than 5 per processor—for example, if you have 4 cores in your server, this number shouldn't exceed 20. If it does, then instructions are queuing up faster than your processors can process them. In this case, you need faster processors or more cores.
Memory\Available MBytes	How much memory is available to use; should be above 100MB. When your server is starved of memory, you'll see decreased performance on the server as memory pages are swapped to disk and reused. In this case, you should increase the server's memory.
Memory\%Committed Bytes in Use	Percentage of committed memory being used. If it rises above 90 percent, your memory usage is heavy and you might need additional RAM. Committed memory is memory that's physically backed by either RAM or pages on disk; this is literally memory that can be used immediately if the server tries to write to it. When committed memory is 90 percent utilized, you're getting dangerously close to the system commit limit. As the number approaches 100 percent, Windows will begin to behave in unexpected ways because processes will be unable to use the memory they need.
Memory\Page Reads/sec	How much memory is being read from disk because of memory pages not being in RAM; should be less than 100. This counter can be used to determine whether you need additional RAM. Windows's Memory Manager automatically determines what stays in RAM and what gets paged to disk. Memory that's used frequently tends to stay in RAM; so when you see heavy page reads, memory pages are being swapped to disk out of necessity rather than for performance reasons.
Network Interface\Bytes Total/sec	Total rate at which the network adapter is processing data; should be below 7 percent of the speed of the network adapter—for example, with a 1Gbps adapter, it shouldn't exceed 9,175,040 bytes.
Network Interface\Packet Outbound Errors	Number of outbound packets with errors; should be 0. If not, you might have a problem with a network adapter. In this case, ensure that the driver is up-to-date first. If the problem continues, consider replacing the network card.

you'd have if you were logged on to the Client Access server directly. However, these tools have some restrictions—perhaps the biggest of which is that they can be installed only on 64-bit workstations. If your administrators are running 32-bit Windows clients or Windows XP, this remote management strategy won't work. However, if you're running a 64-bit client OS on Windows Vista SP2 or later or a 64-bit server OS on Windows Server 2008 R2 or Windows Server 2008 SP2, then you can install Exchange Management Tools. To install the tools, run setup.exe from the Exchange installation media, perform a custom install, and select Exchange Management Tools, as Figure 1 shows. Alternatively, you can use an unattended installation method to install the tools. Enter the following command:

```
setup.com /role:ManagementTools
```

The second option is to use remote PowerShell. Exchange 2010's remote PowerShell capability lets you connect remotely from any workstation that has PowerShell 2.0 and Windows Remote Management (WinRM) 2.0 installed. You can then remotely run EMS commands on your Client Access servers. One of the advantages of using this approach is that you can manage your Client Access servers from a 32-bit client. The range of supported Windows client versions is also broader with this method because remote PowerShell can be used on OSs as old as XP and even Windows Embedded. Both PowerShell 2.0 and WinRM 2.0 are available in the Windows Management Framework Core package that you can download from support.microsoft.com/kb/968929. Windows Management Framework Core can be installed on either 32-bit or 64-bit client OSs that are running XP SP3, Windows Vista SP1, or later.

After you install Windows Management Framework Core, you can use PowerShell 2.0 to establish a remote connection to your Client Access servers

through the remote PowerShell virtual directory. When you connect with PowerShell remotely, your client loads the cmdlets that your account has access to and lets you run them from your workstation. These cmdlets actually run on the Client Access server in the back end, but it appears as if they're running from your workstation. Assuming that you're logged on to a computer in the domain and that you have SSL enabled on your PowerShell virtual directory, you can use the following commands from the PowerShell console on your workstation to connect remotely:

```
$Session = New-PSSession
  -ConfigurationName Microsoft
  .Exchange -ConnectionUri https://
  contoso-ex01.contoso.com/
  PowerShell/ -Authentication
  NegotiateWithImplicitCredential
Import-PSSession $Session
```

Monitoring Performance and Diagnostics

When monitoring your Client Access servers, you want to make the process as automated as possible. Having to log on and manually check the state of servers is time consuming and unnecessary. Several monitoring products are available, including Microsoft System Center Operations Manager and Quest Software's Spotlight on Messaging. If you want to monitor your Client Access servers without third-party software, you can use Windows's built-in tools—but you must be disciplined enough to be proactive about monitoring. You need to keep an eye on several things as you monitor your Client Access server infrastructure.

Exchange administrators often jump straight into advanced diagnostic or troubleshooting tools when a problem arises. However, you should monitor your Client Access servers' Windows event logs because these logs can act as an early alert system that something is wrong. Exchange writes events to the application log. You should also monitor the system logs for warnings and errors that pertain to the underlying OS. Sometimes the error is with Windows Server rather than Exchange. In particular, you want to keep an eye out for events that pertain to the Client Access protocols, Autodiscover, and the address book. When issues exist on servers hosting the Client Access role, these are the common problems areas. Anything IIS related can affect access for clients over Outlook Web App (OWA), Exchange ActiveSync, Exchange Web Service, and Outlook Anywhere, so it's important to keep IIS healthy. RPC Client Access errors don't manifest themselves through IIS, so you should deal with error events that have MSExchange as the event source as soon as possible.

Another thing you need to monitor is your Client Access servers' performance. You should collect information about hardware and services to ensure that they're operating within healthy thresholds. You can use the Performance Monitor tool, perfmon.exe, to collect this information. Performance Monitor uses counters that Exchange Server makes available.

You'll want to monitor aspects of the hardware performance, as well as Client Access server service endpoints. Table 1

Table 2: Performance Counter Objects for Client Access Server Service Endpoints

Service or Virtual Directory	Counter Object
Address Book Service	MSExchangeAB
Availability Service	MSExchange Availability Service
Exchange ActiveSync	MSExchange ActiveSync
Exchange Control Panel	MSExchange Control Panel
Outlook Anywhere	RPC/HTTP Proxy
Outlook Web App	MSExchange OWA
RPC Client Access	MSExchange RpcClientAccess

Table 3: Performance Counters for Client Access Server Service Endpoints

Counter	Notes
MSExchangeAB\NSPI RPC Requests Average Latency	Average time that a 60-second sample of NSPI requests completed in; should be under 1 second, or 1,000 milliseconds.
MSExchange Availability Service\Average Time to Process a Free Busy Request	Average number of seconds that a free/busy request takes to complete; should be under 5 seconds.
MSExchange ActiveSync\Requests Queued	Number of ActiveSync HTTP requests that are queued and waiting for a thread; should be under 100.
MSExchange Control Panel\Requests—Average Response Time	Number of milliseconds that it takes the Exchange Control Panel to respond to a request; should be under 6 seconds, or 6,000 milliseconds.
RPC/HTTP Proxy\Number of Failed Back-End Connection Attempts Per Second	Number of failed connections (per second) that the Outlook Anywhere component is experiencing when trying to connect to the mailbox server; should be 0.
MSExchange OWA\Average Search Time	Amount of time in milliseconds that searches are taking to complete in OWA; should be under 5 seconds, or 5,000 milliseconds.
MSExchange RpcClientAccess\RPC Averaged Latency	Average RPC latency for the latest 1,024 packets; should be under 250 milliseconds.
MSExchange RpcClientAccess\RPC Requests	Number of requests being handled by the RPC Client Access component; should be under 40. A higher number indicates that you might need additional Client Access servers to account for the RPC Client Access load.

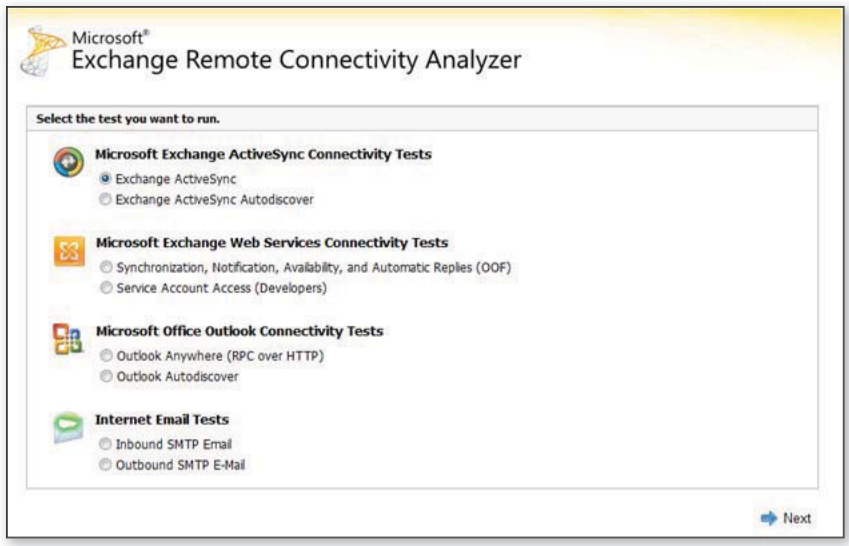


Figure 2: Exchange Remote Connectivity Analyzer

identifies a few key counters to consider when monitoring hardware performance. Table 2 outlines the performance counter objects that are associated with Client Access server service endpoints.

Each Client Access server service endpoint has unique needs, so one performance threshold won't apply to all services. For example, latency has a higher threshold in ActiveSync monitoring than in RPC Client Access monitoring. Table 3 outlines some important performance counters to monitor for these services and virtual directories.

Troubleshooting Client Connectivity

Because the Client Access role's main functionality is to provide client connectivity, the majority of the problems you encounter with the Client Access server are related to clients not connecting as expected. When you experience client connectivity failures, you should attempt to isolate the problem and determine whether the problem is really with the Client Access server or if it could be on the client's end.

Remote connectivity testing. One of the easiest ways to test connectivity is to use the Exchange Remote Connectivity Analyzer, found at www.testexchangeconnectivity.com. This online connectivity test tool, which Figure 2 shows, is maintained by Microsoft and can help determine whether a problem is with the client's connection or with the Exchange server.

Connectivity test cmdlets. Exchange includes several cmdlets that you can use to test various aspects of the Client Access server for connectivity problems. Table 4 lists these cmdlets and explains what each of them does.

The connectivity test cmdlets use a preconfigured mailbox to run tests against various virtual directories on the Client Access server. Before you can run the tests, you must generate the account for the cmdlets to use. To generate this account, you use the PowerShell script called New-TestCasConnectivityUser.ps1. You can find this script in the Scripts folder of your Exchange installation path, which by default is C:\Program Files\Microsoft\Exchange Server\V14\Scripts. You can run the script without any parameters, or you can specify the organizational unit (OU) for the account and its Unified Messaging

Table 4: Connectivity Test Cmdlets

Cmdlet	What Is Tested
Test-ActiveSyncConnectivity	Tests ActiveSync mobile device connectivity. You can specify the mailbox in the command, and the cmdlet will attempt a full synchronization with it.
Test-EcpConnectivity	Checks access to the Exchange Control Panel virtual directory that's hosted on the Client Access server specified in the command.
Test-ImapConnectivity	Tests the ability of IMAP4 clients to connect to their mailbox.
Test-MapiConnectivity	Determines whether a mailbox can be logged on to. You can run this command against a database to test the system mailbox for that database.
Test-OutlookConnectivity	Runs a series of Outlook tests, including profile creation, configuration via Autodiscover, and access to the mailbox.
Test-OutlookWebServices	Tests Autodiscover to verify that the configuration being returned is correct. Each returned service endpoint is also tested.
Test-OwaConnectivity	Checks OWA to determine whether it can be contacted and logged on to.
Test-PopConnectivity	Tests the ability of POP3 clients to connect to their mailbox.
Test-PowerShellConnectivity	Tests that remote PowerShell works and can successfully issue commands.
Test-WebServicesConnectivity	Checks the functionality of Exchange Web Services through the use of Outlook Anywhere.

Learning Path

See the other articles in this series:

"Exchange Server's Client Access: An Introduction," InstantDoc ID 125061

"Exchange Server's Client Access: Deploying Your Servers," InstantDoc ID 125347

"Exchange Server's Client Access: Load Balancing Your Servers," InstantDoc ID 125863

"Exchange Server's Client Access: Securing Your Servers," InstantDoc ID 128939

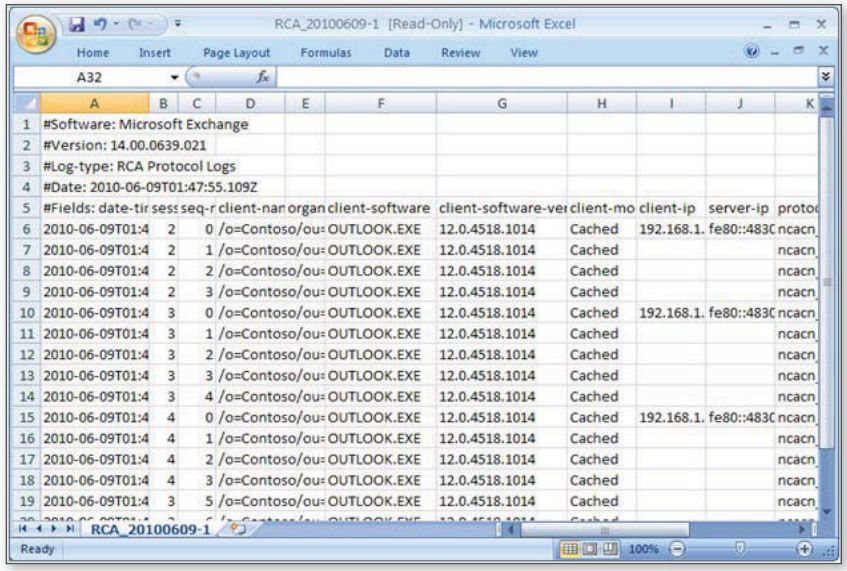


Figure 3: Protocol logs for the RPC Client Access service

Table 5: Enabling Protocol Logging for the Client Access Server Services

Service	How to Enable
RPC Client Access	Edit the XML file named Microsoft.Exchange .RpcClientAccess.Service.exe.config in the Exchange Server\V14\bin folder. Ensure the following line is included under the <appSettings> element: <add key="ProtocolLoggingEnabled" value="true"/>
Address Book Service	Edit the XML file named Microsoft.Exchange .AddressBook.Service.exe.config in the Exchange Server\V14\bin folder. Ensure the following line is included under the <appSettings> element: <add key="ProtocolLoggingEnabled" value="true"/>
POP3 Service	Run the following command in EMS: Set-PopSettings -ProtocolLogEnabled $true
IMAP4 Service	Run the following command in EMS: Set-ImapSettings -ProtocolLogEnabled $true

settings. When you create the account, you're prompted for a one-time password. You never need to know this password again because Exchange manages it after the account is created and because it's changed on a regular basis.

Diagnostic logging. To troubleshoot at a level deeper, you can turn on diagnostic logging for several Client Access server components. Exchange 2010 provides an interface to use in EMC. You can access the diagnostic logging interface for Client Access servers by selecting Server Configuration, Client Access. Choose the Client Access server that you want to enable logging on and select Manage Diagnostic Logging Properties from the Actions pane. The logs generated from the diagnostic logging process are written to the Application log in the Windows event logs.

Protocol logs. The RPC Client Access, Address Book, IMAP4, and POP3 services all offer the ability to turn on protocol logging. Protocol logging lets you see the conversation between the client that's trying to connect and the Client Access server that's responding. These logs are stored as comma-separated files that can be opened in any text editor. Some of the information in the protocol logs is common across all the services, and some of the information is unique to the service you're logging. Figure 3 shows the protocol logs for the RPC Client Access service. Note that this log contains some valuable information that's specific to RPC Client Access troubleshooting, such as the client software (outlook.exe), the version (12.0.4518.1014), and even which mode it's running in (cached).

Protocol logging is enabled on these services either through the service's configuration file or through EMS. The default location for the logs is C:\Program Files\Microsoft\Exchange Server\V14\Logging. Table 5 describes how to enable the protocol logs.

For client protocols that use IIS (OWA, Exchange Control Panel, Exchange ActiveSync, Exchange Web Service, Autodiscover, Outlook Anywhere, and remote PowerShell), you can use the IIS logs to gather similar log information. By default, these logs are in the folder C:\inetpub\logs\LogFiles. Logging in IIS is enabled by default, so no additional configuration is necessary to use these logs.

Go Forth and Administer

Client Access servers comprise only a single piece of your overall Exchange infrastructure—a lot of the focus in Exchange administration leans toward data administration on mailbox servers. Administering Client Access servers doesn't require a lot of time or attention, but you can spend a lot of time troubleshooting if something goes wrong. To prevent little problems from turning into large outages, you should proactively monitor and troubleshoot your Client Access servers.

In this series I walked you through various aspects of the Client Access server role in Exchange 2010 to help you better understand what it does and how to work with it. The information I provided in the series will help you effectively deploy and manage a common Client Access server implementation.

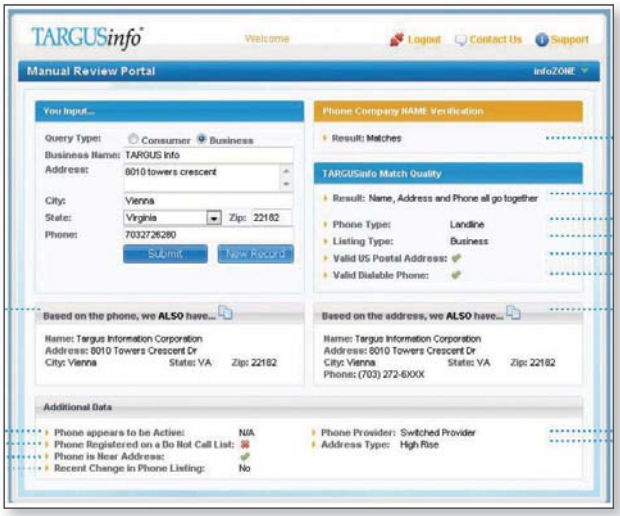
InstantDoc ID 129254

Ken St. Cyr
(ken.stcyr@microsoft.com) is a solution architect at Microsoft with more than 10 years of industry experience. He's a Microsoft Certified Master in Directory Services and the author of *Exchange Server 2010 Administration Instant Reference* (Sybex).

Linoma Software Releases GoAnywhere Director 3.5

Linoma Software has released **GoAnywhere Director 3.5,** a managed file transfer solution that automates and secures data exchange with your customers, trading partners, and enterprise servers. New features in GoAnywhere Director 3.5 include integration with enterprise message queue services; providing access to files and folders on Windows, Linux/Unix, and IBM i servers; wizards to set up monitors that scan for file updates; automatic resume for file transfers after a connection break; file locking; command shortcuts; and integration with SQL Server, MySQL, and DB2 for IBM i for high availability. To learn more, visit www.goanywheremft.com.

TARGUSinfo Launches On-Demand Email Verification



TARGUSinfo has announced **On-Demand Email Verification,** an extended verification solution. The new offering lets businesses identify the probability of a connection between an email address and an individual. The traditional approach to email verification attempts to validate syntax, domain, and username. TARGUSinfo's verification solution provides these basic checks and also verifies correlations between email address and other identifiers associated with an individual, such as name, address, and phone. To learn more, visit www.targusinfo.com.

PRODUCT SPOTLIGHT

Acer Unveils Server and Storage Solutions

Acer has announced a comprehensive line of server and storage solutions. Acer's server and storage products include tower, rack, blade, and multi-node solutions that are based on Intel Xeon and AMD Opteron processors. Benefits of the new servers cited by the vendor include offerings built on open, industry standard architectures; vertical manufacturing and configuration integration; development leadership in virtualization and multi-node architectures; 24/7 phone support; and more.

The product lines include the Acer tower server line, the Acer rack server line, the Acer rack multi-node server line, the Acer blade server line, and the Acer Network Attached Storage line. These server and storage solutions support Windows Server 2008 R2 SP1 and Hyper-V. Acer provides storage solutions for its server offering through a partnership with Hitachi Data Systems that integrates storage solutions into Acer's server offerings.

"Acer has steadily built one of the broadest lines of server and storage solutions in the world and now we are bringing this offering to the US to meet customer demands for cost-effective performance, simplified management, flexible scalability, and return on storage investments over time," said Gianluca Degliesposti, vice president of worldwide business development for Acer Servers and Storage. "Our initial family of 16 server solutions also leverages our deep expertise in virtualization, multi-node architectures, and HPC to meet increasingly challenging needs in cloud computing and other complex computing applications. We plan to further expand our family this year to meet additional customer needs across the full range of server and storage environments."

For more information and pricing, visit www.acer-group.com.

Gemalto Launches Protiva One Time Password Application for Mobile Users

Gemalto has introduced **Protiva Mobile One Time Password** (OTP), a new way for businesses and their employees to deploy two-factor authentication using their mobile phones. OTP replaces static passwords with strong authentication and provides an additional level of security for transactions and access control. To gain access to company resources, employees use both a mobile credential and their username and one-time password. Protiva Mobile OTP works with BlackBerry and iOS. To learn more, visit www.gemalto.com.

Remote Support for Android Tablets and Smartphones

LogMeIn has announced remote support for Android tablets and smartphones via **LogMeIn Rescue.** The product includes a diagnostic dashboard that provides device information, the ability to transfer files between the technician and the end user device, and the ability to chat with the user. There are two versions of the product

available—the mobile operator version also allows for remote control. To learn more, visit secure.logmein.com.

Origin Storage Launches Encryption for Laptops

Origin Storage has announced **Enigma FIPS,** a series of notebook hard drives designed for Dell notebooks that incorporate the Seagate Momentus Self-Encrypting Drive that has recently secured FIPS 140-2 certification from the National Institute of Standards and Technology. The Momentus drive provides hardware-based encryption without performance degradation. The FIPS 140-2 solution is the latest in the Enigma range to provide organizations of all sizes with a quick and cost-effective way to secure laptops using high levels of hardware encryption. To learn more, visit www.originestore.com.

Applications Manager Adjusts Virtual Infrastructure Resources

ManageEngine has announced automated provisioning of virtual resources with **ManageEngine Applications Manager,** the company's server and application performance monitoring software. Applications Manager will automatically add, start, or stop virtual machines in a VMware ESX/ESXi server farm when the number of active sessions in a server exceed a specified threshold. According to the vendor, Applications Managers lets IT pros utilize their virtual resources more effectively and cut operational costs. To learn more, visit www.manageengine.com.

Paul's Picks

www.winsupersite.com

SUMMARIES of in-depth product reviews on Paul Thurrott's SuperSite for Windows

Moving to Solid State Disk

PROS: Dramatically better all-around performance; somewhat better battery life on the same hardware when compared to a traditional hard drive

CONS: Expensive; small capacities

RATING: ◆◆◆◆◇

RECOMMENDATION: Solid state disks (SSDs) are more expensive and currently ship in much smaller storage capacities than their more traditional spinning-disk hard-drive brethren. So although 2TB desktop hard drives can be had for well under $100 at traditional retailers like Amazon.com, smaller-capacity SSDs cost much more, usually more than $200 for a 120GB drive. Why would you want to replace a cheap high-capacity hard disk drive (HDD) with an expensive low-capacity SSD? Speed. SSDs aren't just faster, they're dramatically faster. Windows 7 installs in under 10 minutes, and on a mainstream Core 2 Quad-based desktop, boots in about 15 seconds.

CONTACT: Intel • www.intel.com • OCZ • www.ocztechnology.com

DISCUSSION: www.winsupersite.com/article/windows-7/The-Great-SSD-Migration-Part1-Migrating-a-Windows-7-Desktop-to-SSD.aspx

Mac OS X "Lion" Developer Preview

PROS: Only one OS X product version; simpler, touch-friendly controls; simpler app discovery

CONS: iOS-like app launcher is perhaps too basic; window management tools are complex

RATING: ◆◆◆◆◇

RECOMMENDATION: Apple has borrowed some interesting ideas from iOS (the basis of its iPhone, iPod Touch, and iPad) for its next OS X version, Lion. It's reducing the number of product versions to one: OS X Server will be bundled with the desktop version and installed like a feature. OS X's multi-touch features have additional gesture support and more window management functionality, and an alternative app-launching scheme based on the grid of icons from iOS. The current developer preview strongly hints at where Apple's heading. I can't wait to see which of these features Microsoft, um, is inspired by for Windows 8.

CONTACT: Apple • www.apple.com

DISCUSSION: www.winsupersite.com/article/windows-7/What-Microsoft-Can-Learn-From-Mac-OS-X-Lion.aspx

InstantDoc ID 129976

REVIEW

Stratus ftServer 4500

Most organizations aspire to high availability. However, high availability typically comes at the cost of implementing highly complex and difficult-to-manage solutions, such as Microsoft's failover clustering. Stratus Technologies' Stratus ftServer 4500 is a high-availability server that can provide five 9s of availability with very little added complexity.

Much like the NEC 5800 unit that I reviewed earlier this year (see "NEC Express5800/R320," February 2011, InstantDoc ID 128943), the Stratus ftServer 4500 is a 4U rack-mounted server that provides dual copies of all system components. In other words, there are two motherboards, two sets of CPUs, and two sets of RAM and storage. Each of these sets is contained in its own 2U unit. Stratus calls each unit a CPU-I/O Enclosure. Each of these CPU-I/O Enclosures slides into a shared rack-mounted chassis. The two CPU units run in lockstep, with the current memory and CPU instructions shared between each of the two CPU-I/O Enclosures. Figure 1 shows the Stratus ftServer 4500.

From when I first opened the shipping container, it was apparent that the Stratus ftServer is in a league apart from ordinary servers. Instead of arriving in a plain corrugated box, the Stratus 4500 arrived on a pallet. The Stratus ftServer shipped in three main pieces: two CPU-I/O Enclosures and one industrial-strength steel chassis. These components were quite heavy, so the ftServer installation took a little doing. To install the unit, I first installed the chassis into my server rack and then slid each of the CPU-I/O Enclosures into the chassis. I used thumbscrews at the front of the unit to secure the CPU-I/O Enclosures. The chassis provides internal connectors that are used to plug in each CPU-I/O Enclosure. These connectors are how the CPU-I/O Enclosures communicate and stay in sync.

The Stratus ftServer 4500 that I tested came equipped with two logical Intel Xeon E5504 quad-core CPUs running at 2GHz. The system also made use of the Intel 5500 chipset. The unit that I tested came configured with 16GB of RAM and

Figure 1: Stratus ftServer 4500

136GB of Serial Attached SCSI (SAS) disk storage spinning at 15,000rpm. In the case of this system, the key word is *logical* because the ftServer actually has two physically matching sets of CPU, motherboard, RAM, and disk storage—one set per CPU-I/O Enclosure. This duplication of system components is what enables the fault tolerance. Each CPU-I/O Enclosure can support up to 96GB of RAM running at 800MHz and up to 4.8TB of SAS disk storage.

Internally, each CPI-I/O Enclosure had two PCI Express 2.0 expansion slots and four more optional PCI Express 1.0 or PCI-X expansion slots. On the back of each CPU-I/O Enclosure, there were three 1GB network ports. Two of the network adapters were intended for client networking activity, whereas the other network adapter was reserved for remote management. Each CPU-I/O Enclosure also had an additional two-port 1GB network adapter. Between both of the CPU-I/O Enclosures, there were eight client network ports, which were configured as a team using Intel's Advanced Network Services (ANS) technology. This teaming technology provides networking fault tolerance.

Each CPI-I/O Enclosure in my test unit also had a Fibre Channel adapter. The connections for the video display, keyboard, serial ports, and USB ports were on the chassis—not on each CPU-I/O Enclosure. The video used a standard nine-pin VGA port. An integrated video controller provided 8MB of RAM and supported a maximum of 1024 × 768 display resolution. Notably, the Stratus ftServer 4500 had no PS/2-style mouse and keyboard ports. The mouse and keyboard connections are USB only; you can use the port on the front of the unit or the three USB ports on the back of the unit. Because two of these ports are required by the mouse and keyboard, I wished the unit had more USB ports available—especially on the front of the system. The front of the chassis also provided a vertically mounted DVD-RW drive.

The Stratus ftServer 4500 that I tested came with Windows Server 2008 R2 x64 Enterprise Edition preinstalled. You can also order it with VMware vSphere 4 or Red Hat Enterprise Linux (RHEL) 5.

Despite its fault-tolerant configuration, managing the system was essentially the same as managing a standard Windows Server system. All the management tools that you typically use, such as Control Panel, Services, Event Viewer, and Device Manager, were essentially just like you'd expect. In addition, there was an ftServer Management Tools icon on the desktop that lets you work with the fault-tolerant configuration. The Stratus ftServer 4500 provides a remote-management facility called the Virtual Technician Module

Michael Otey | motey@windowsitpro.com

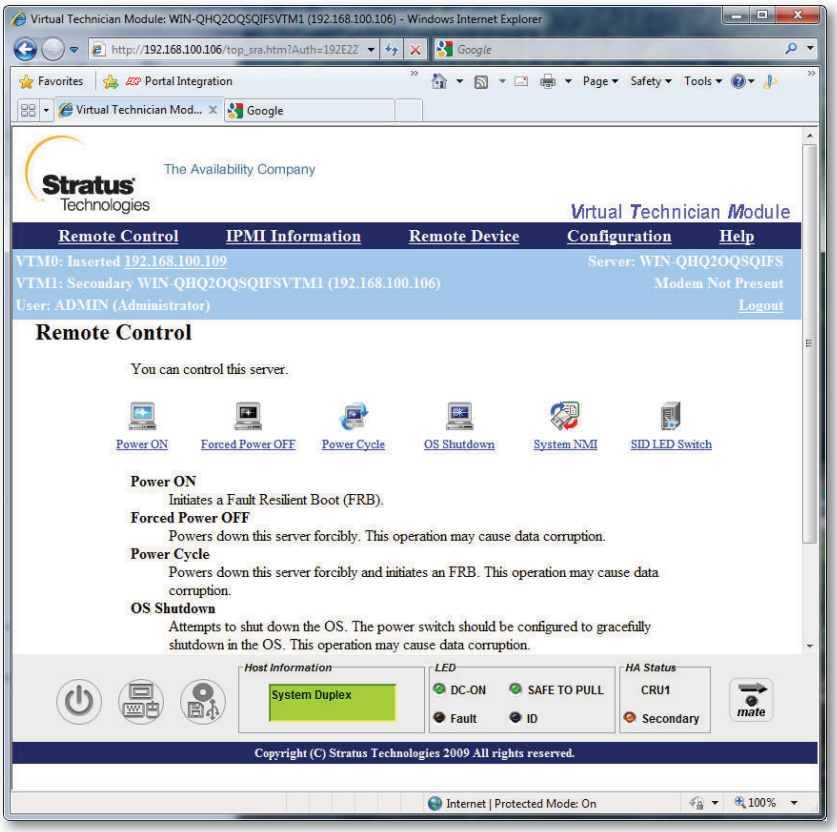


Figure 2: Virtual Technician Module

(VTM), which Figure 2 shows, that lets you manage the system remotely. Notably, the VTM lets you power the server on and off. The VTM works even when the system is in a powered-down state, because as long as the system is connected to power it never completely powers off. At idle state, the system consumed about 53W.

To test the system, I configured four Microsoft Hyper-V virtual machines (VMs). Each VM was running SQL Server 2008 Enterprise Edition and a single instance of SQL Server 2005 Enterprise Edition. The VMs were configured to use 512MB of RAM, and the VM files were stored on the local drives. This test suite consisted of a mixed workload of database queries. The database tests ran a set of 27 queries against each virtual SQL Server instance. The Stratus ftServer 4500 proved to be an excellent performer, with test scores comparable to those of the other high-end servers we've tested in the *Windows IT Pro* labs.

When the system is running in fault-tolerant mode, there's a *Ready to Pull* light that's lit on the front of the unit. To test the ftServer's fault-tolerant capabilities, I pulled the plug out of the back of each of the units while the system was running the test workload. In addition, I tried removing the network cables from one of the units, as well as pulling out the hot-swappable drive. In all cases, the unit lived up to its five-9s reputation and continued to function with no end-user interruption. The ftServer 4500 continued running the workload with no noticeable slowdown and absolutely no interruption of services.

After I reconnected the power to one of the CPU-I/O Enclosures, the unit took a few minutes for the two CPU modules to resynchronize. Again, the workload continued to run with no interruption and no noticeable slowdown. The resynchronization process was completely automatic, and there was no manual intervention necessary.

The time required for synchronization depends in part on the workload the unit is handling. Under heavy workload, the resynchronization took about 10 minutes. When the system was idle, the resynchronization completed in about a minute. During the resynchronization period, the unit wasn't fault tolerant, and I needed to wait until the *Ready to Pull* light was relit to perform another test. When the *Ready to Pull* light came back on, the ftServer 4500 was once again fully fault tolerant. While running under the workload generated by our virtualization test suite, the unit consumed about 574W.

A unique availability feature in Stratus's series of computers that goes way beyond the availability offerings from most vendors is Stratus's ActiveService technology. ActiveService lets the server automatically contact Stratus support and even automatically order replacement parts if a hardware failure is detected. Stratus informed me that replacement parts are shipped next-day. I didn't experience any real hardware failures during the 3-month testing period, but I did run across a couple of problems during testing, related to misconfiguring the unit. Stratus's support provided expert help and was able to resolve my issues quickly. ActiveService customers have 24 × 7 support, and support personnel can connect to the server remotely for problem remediation.

Overall, I found the Stratus ftServer 4500 an excellent choice for a high-availability server. The ftServer 4500 brings five 9s of availability, at a price that's within the reach of most businesses. In addition, managing the unit is almost the same as managing a standard server. If you're in the market for a new server for a mission-critical workload, or you're looking into other high-availability technologies, I highly recommend the Stratus ftServer 4500.

InstantDoc ID 129998

Stratus ftServer 4500

PROS: Reliable; easy to manage; excellent scalability; rugged construction

CONS: Costs more than a standard server; could use more USB ports on the front of the unit

RATING: ◆◆◆◆◆

PRICE: Starts at $31,231, including Windows Server 2008 R2 Enterprise; $40,672 as tested

RECOMMENDATION: The Stratus ftServer 4500 is an excellent choice for high availability; it provides five 9s of reliability and is no more difficult to manage than a standard server.

CONTACT: Stratus Technologies • 800-787-2887 • www.stratus.com

REVIEW

GroupID

After seeing a demo of Imanami's GroupID, I was keen to get my hands on the product to see if it could really solve common identity management problems that most Windows shops face, without adding huge amounts of complexity. GroupID supports Windows Server 2003 and later and Exchange Server 2003 and later. GroupID consists of four modules: Synchronize, Automate, Self-Service, and Reports—which I'll deal with separately for the purposes of this review.

Synchronize. The GroupID Synchronize module lets you keep Active Directory (AD) up-to-date by synchronizing information from other data sources, such as Oracle and Microsoft SQL Server databases, LDAP-compatible directories, and text files. You can use the simple wizard to map fields from your data source to AD. In addition, you can use built-in rules or create your own VBScript solutions to perform simple data transforms. GroupID Synchronize includes the ability to preview synchronization and transform results before running a job. You can also configure email alerts.

Unlike one of its main competitors, Microsoft Forefront Identity Manager, GroupID doesn't use a metaverse, a repository where data is stored, merged, and transformed before being distributed to connected directories. GroupID Synchronize performs transforms on the fly—but the lack of a metaverse makes GroupID less flexible in terms of merging data from multiple directories. However, GroupID's simple approach will likely be a benefit for many organizations, and its functionality is more than adequate except for the most complex systems.

Automate. The Automate module provides semi to fully automatic AD group management functionality. Based on user information held in AD, GroupID Automate can use LDAP queries to create and update AD security groups (i.e., Smart Groups) or distribution lists (DLs). A service runs on the machine on which GroupID is installed and periodically updates group membership. GroupID comes with a set of PowerShell cmdlets for command-line automation.

GroupID Automate introduces several new group security concepts to AD. Private Groups are assigned to an owner, and group membership can be managed only by that person. Semi-Private Groups are similar to Private Groups, with the exception that users can send membership requests to the owner. No permission is required to leave or join Public Groups. Finally, Semi-Public Groups are similar to Public Groups, but email notifications are sent to the group owners as membership changes.

DLs and security groups can be expired, either manually or automatically after a set period of time. All groups created in GroupID are assigned the default expiration policy, but policies can be modified on a per-group basis. When a group is expired, initially it's only marked as such, then deleted after a period of time that's set in GroupID's system configuration. SQL Server is required to expire security groups.

Dynasties in GroupID can be thought of as Smart Groups on steroids that are used to create and manage one or more child groups based on given criteria. Child groups are automatically populated under a parent Dynasty group and inherit the parent's properties, such as group type and security settings. A query is created to determine who should be members of the child groups, but Dynasties differ from standard Smart Groups with an additional parameter, the *group-by* field, by which Dynasties determine how to split up the results of the query into separate child groups. For instance, you can create multiple groups in a Dynasty based on an LDAP query to list all HR managers and have the results split into multiple child groups based on a *group-by* field, such as Office (or physicalDeliveryOfficeName, as it appears in the AD schema). This would result in *x* number of groups because there are different user accounts in different offices in the returned LDAP query. Dynasties are useful for creating and managing DLs, but the logic can also be applied to security groups. Dynasty templates are included for some common scenarios, and multi-level Dynasties are also supported.

Self-Service. GroupID Self-Service provides one or more web portals for users to manage directory data and group memberships in AD. Considering that it can be costly to service calls to the Help desk, giving users the ability to manage groups without intervention from IT can be cost effective. Self-Service works in conjunction with the additional security descriptors that Automate adds to AD: Public, Semi-Public, Private, and Semi-Private.

Users can request membership to groups, and owners can manage those requests via the web portal. Self-Service supports workflows so that changes to AD information can be approved before being committed. Self-Service also supports anonymous or authenticated read-only access to the directory for the purposes of retrieving information to share via a spreadsheet or distribute to portable devices.

Reports. GroupID Reports is a free module that lets administrators generate reports on user, group, and computer objects in AD. Reports can be output in HTML, XLS, and XML formats. A variety of built-in reports can be tailored according to your needs.

Accurate data is the key. AD rarely serves as an authoritative source of employee information, which limits its worth in terms of effectively managing security and communication via DLs. In organizations with 250 employees or more, GroupID can help fully realize the potential of AD and Exchange.

InstantDoc ID 129859

GroupID

PROS: Simple implementation; wide range of functionality

CONS: Confusing user manual

RATING: ◆◆◆◆◇

PRICE: From $3 to $20 per seat, based on number of modules and volume

RECOMMENDATION: GroupID is a good fit for organizations looking for an effective identity management solution that won't break the budget or add unnecessary complexity.

CONTACT: Imanami • 800-684-8515 • www.imanami.com

Russell Smith | rms45@rsitc.com

Cisco ASA 5505

Many small businesses, as well as organizations with branch offices, rely on broadband routers to act as firewalls to protect their networks. Unfortunately, these devices—especially those provided by the broadband provider—aren't true firewalls and rely on Port Address Translation (PAT) or Network Address Translation (NAT) to protect connected computers. Although some broadband routers have rudimentary firewalls, they're often insufficient or they lack the enterprise-class features that branch offices require. For these reasons, I recommend that you look at the range of Adaptive Security Appliances (ASAs) from Cisco, which are the successors to the PIX family, and are excellent firewalls.

The Cisco ASA 5505 is the entry-level product in the family, but it's packed with enterprise-class features that can be used as organizations grow or their needs change. As in many Cisco products, the ASA 5505's advanced features need licenses to unlock them for use. A basic-level license supports 10 simultaneous users on the LAN, 10 IPsec VPN connections, and 2 SSL VPN connections. This configuration will cost you less than $400 and is sufficient for most small networks. The ASA 5505 can be purchased with licenses for 50 users, an unlimited number of users, more VPN peers, failover support, Virtual LANs (VLANs), and a true demilitarized zone (DMZ) LAN segment, among other features. You can also purchase upgrade licenses later if you require them. All the ASA 5505's features and licensing options can make your head spin.

The ASA 5505 comes with two network cables, a console port cable that connects to a serial port on a PC, and a power supply. When you unpack the ASA 5505, the chassis might look familiar and remind you of other Cisco products that are tailored to small businesses. (To keep costs down, Cisco standardized its chassis design.) Figure 1 shows the Cisco ASA 5505. The front of the ASA 5505 has a USB port for future expansion, and the back of the device has a card slot for expansion cards, eight Fast Ethernet (100Mbps) network ports, a console port, and a power connection. Of the network ports, port 0 is configured by default to connect to the Internet, and ports 1 through 7 are configured as LAN ports. Ports 6 and 7 provide Power over Ethernet (PoE). Connect port 0 to your Internet connection, connect your LAN devices to ports 1 through 7, and connect the power to get started.

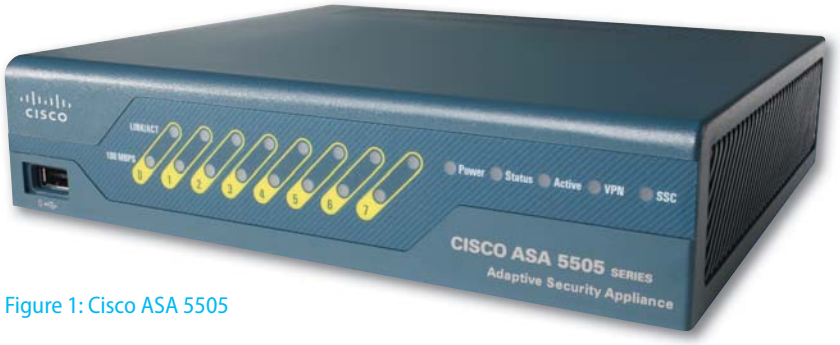


Figure 1: Cisco ASA 5505

Initial configuration is a breeze. Open your browser and enter https://192.168.1.1/admin to get access to the Cisco Adaptive Security Device Manager (ASDM) and run the ASDM Startup Wizard. Note that you must install Java to run the ASDM. The ASDM Startup Wizard will ask you a few questions and configure your ASA 5505. The simplest configuration is for the ASA to use DHCP to obtain an IP address from your ISP, as well as for the ASA to function as a DHCP server to your internal network and to use PAT.

The one glitch in configuration is that the ASA 5505 might not ship with the latest firewall software installed (version 8.4.1 at press time). You should receive a CD-ROM with your ASA 5505 that contains the latest software. You can upgrade both the firewall and UI software by using Trivial FTP (TFTP), FTP, and (from an internal website) HTTP. The upgrade process isn't as simple as it could be; you'll need to consult the Cisco documentation to perform the upgrade.

By default, the ASA 5505 blocks all unsolicited incoming traffic to your LAN. If you want to configure VPNs (whether SSL VPNs, VPN tunnels for site-to-site connectivity, or VPNs for remote access), you can use wizards in the ASDM to get them up and running quickly. If you need to publish servers on your LAN to the Internet, you can quickly accomplish that task through the ASDM as well, by adding a public server in the firewall configuration section. The ASDM provides configurations for common protocols and services, making the task quite easy. The ASDM can also be used to monitor your ASA 5505 and to troubleshoot problems. The ASDM is a bit clunky in places, and you might need to spend some time with the online Help and with Cisco's installation guides to configure some of the advanced features.

The Cisco ASA 5505 is a great firewall with enterprise features that won't break the bank, especially for small-to-midsized businesses (SMBs). This appliance provides peace of mind and can grow with your company and needs.

InstantDoc ID 129791

Cisco ASA 5505

PROS: A real firewall with enterprise-class features; easy setup and configuration; flexible licensing

CONS: Updating software isn't easy; confusing array of layered features and licensing; somewhat clunky UI

RATING: ◆◆◆◆◆

PRICE: $370 for 10 users; $525 for 50 users; $620 for unlimited users; additional license options available

RECOMMENDATION: This product is ideal for small offices and home offices, as well as branch offices of midsized organizations.

CONTACT: Cisco Systems • 800-553-6387 • www.cisco.com

John Howie | jhowie@microsoft.com

REVIEW

ShadowProtect Server

When I first heard of ShadowProtect Server, I thought it sounded interesting but that it would probably be very similar to most other backup products. I quickly discovered that ShadowProtect Server is quite a bit more than just another backup product. Although the product performs the typical backup and restore operations that you'd expect from any solution that claims to be a system backup product, what really sets ShadowProtect Server apart is its flexibility during the recovery process and its automated management of the backup files. ShadowProtect Server installs on Windows Server 2008 or Windows Server 2003; you can then remotely install and manage ShadowProtect Desktop from the server.

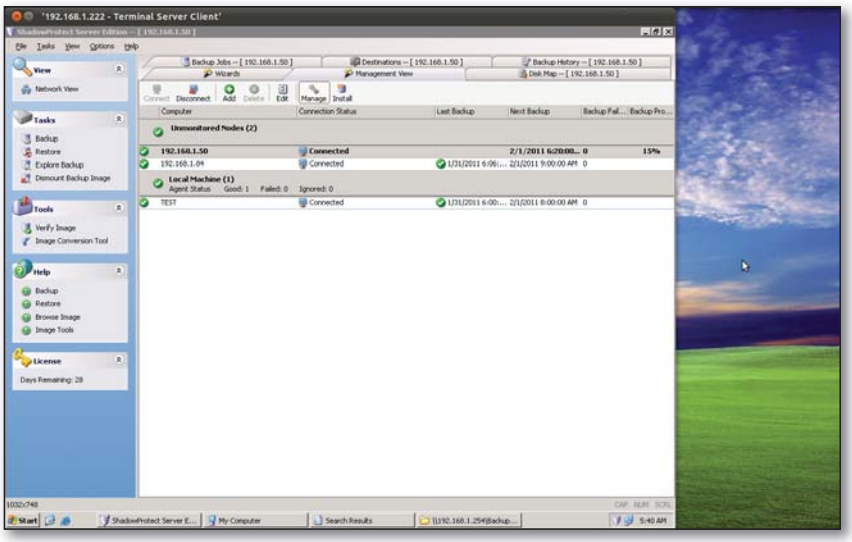


Figure 1: ShadowProtect Server management console

Backup and Recovery

To recover a system, you have the options of a granular file restore, full system restore from bare metal, full system restore from bare metal on dissimilar hardware, or conversion of your backup files to a Microsoft, VMware, or VirtualBox compatible virtual machine (VM). ShadowProtect Server also supports Microsoft Volume Shadow Copy Service (VSS), so you can safely back up servers running applications such as Microsoft Exchange Server 2007 or SQL Server 2005.

Supported backup destinations include local directories and network shares. StorageCraft has done away with tape but suggests two options for tape-like archiving needs. One option is to archive to a locally attached USB drive, then take the drive offsite and lock it in a safe just as you would with tape.

Another option is to keep an online archive by doing a full system backup, physically transport the full backup to a remote site, and place it on a file share. You'd then point a second backup routine at the remote site file share and configure this backup routine to only perform incremental backups to the remote share. This approach avoids the necessity of copying the large full system backup across a WAN link. In addition, incremental backups can be scheduled to be copied across the network without affecting business operations because the incremental backups are a much smaller file size. These incremental backups can be configured to run at any hour of the day and as often as every 15 minutes. You can also configure ShadowProtect Server to send daily and weekly status reports telling you whether each one of the backup jobs completed or failed. As these incremental backups begin to accumulate, you can use the included ShadowProtect ImageManager tool to verify and consolidate your incremental backups down to weekly or monthly backups. By default, ImageManager verifies new backups as they complete; you can specify the number of days before the backups are rechecked. Meanwhile, your onsite backup routine continues creating full backups every week or month, with daily or hourly incremental backups at the same location as the server for quick recovery in the event of a server disaster. Without an automated tool such as ImageManager, I'd recommend archiving these remote files and starting the process over every few months. The idea of using another product without something like ImageManager and having to restore from literally hundreds or possibly even thousands of incremental backups would make me a little uncomfortable.

Testing

To evaluate ShadowProtect Server, I installed the product on my Windows 2003 machine. (Supported server OSs include Windows 2000 Server SP4 through Server 2008 R2.) Installation is a breeze; you simply insert the CD-ROM, select your product, and click Next until the product successfully installs. After the installation completed, I created two shared folders on my server. Then I used ShadowProtect Server to perform a full backup. I added content to both shares from the NAS device and performed an incremental backup. Next, I created a task to email me status reports of backup jobs on a weekly basis. I selected the option to have ShadowProtect Server send a test report and immediately received the status report in my Gmail Inbox. Then, I shut down the server and replaced the Windows 2003 machine's drive with a drive of about the same size.

Next, I booted from the ShadowProtect Server CD-ROM into the graphical StorageCraft Recovery Environment. When you start the StorageCraft Recovery

Nate McAlmond | mcalmond@gmail.com

Environment, you can choose between a Server 2008–based or Windows 2003 environment. Technically, you can use either environment to perform a restore; however, the Windows 2003 environment includes the option to press F6 and load device drivers if necessary. If you're restoring to newer hardware, you'll want to choose the Server 2008 environment because it's more likely to have the necessary hardware drivers. From the Windows 2003 recovery environment I was able to easily map a network drive to the NAS device and start the recovery process. In less than 15 minutes, the recovery process completed and the server (including 8GB of data) was identical to before I exchanged the hard drives.

My next test with ShadowProtect Server was to remotely install and back up a desktop computer. (Supported desktop OSs include Windows 2000 Professional SP4 through Windows 7.) For remote installation, the program requires that you specify the location of the installation and answer file. The installation files and several answer files are included on the ShadowProtect Server installation CD-ROM. The purpose of the answer files is to specify how the installation on the remote computer should occur (i.e., visible to the end user or not). If you choose a completely silent installation, the answer file will include all the possible options for installation.

On my first remote installation attempt on my Windows 7 Home Premium computer, I received an Access Denied error message and wasn't able to continue. After a few minutes on the Knowledge Base section of the StorageCraft website, I had my answer. I turned off User Account Control (UAC), restarted the Windows 7 Home Premium computer, and was able to successfully complete the remote installation. According to the StorageCraft website, this problem shouldn't occur in domain environments because the trust relationship within a domain should prevent UAC from interfering.

At this point I could configure all the backup options for the Windows 7 Home Premium computer from the Windows 2003 ShadowProtect Server console. The only issue to be aware of when configuring a remote computer in this manner is that the computer must be connected to the network and powered up before you can make any changes. Although I understand that this is just how the application works, it would be nice if the setting changes could be pushed to the remote computer later so that you could make configuration changes while the remote computer was disconnected, as in the case of roaming laptops.

Next, I performed a test of ShadowProtect Server restoring to a virtual environment. For this test, I installed Microsoft Virtual PC 2007 on the Windows 2003 computer. I then configured a new VM with a new empty hard drive. While booting the new VM, I attached the physical CD-ROM of the host, which contained the ShadowProtect Server installation CD-ROM, in order to boot the VM into the StorageCraft Recovery Environment. Just like when restoring the physical machine, I used the StorageCraft Recovery Environment GUI to map a drive to the network location that contained the backup files, then I started the recovery process. The recovery process completed within about 45 minutes. After a couple of restarts to finish installing the new VM hardware, the VM was identical to the Windows 2003 physical machine (other than the hardware changes, of course). I assume that the increased recovery time was a result of the VM having significantly less processing power compared with the host machine.

My last test with ShadowProtect Server was a trial of the VirtualBoot restore option. For this technique, you need to install the VirtualBox server virtualization software and ShadowProtect Server on the same machine. You can download VirtualBox for free from www.virtualbox.org. After installation, you should be able to right-click a ShadowProtect Server backup file, select VirtualBoot, and watch the server (now virtualized) start up in a fraction of the regular restore time. However, I ran into some problems. I had downloaded the most recent version of VirtualBox and installed it on my Windows 2003 machine that was already running ShadowProtect Server, but the restore option failed. After multiple failed attempts, I decided to take a look at StorageCraft's online Knowledge Base. My problem was that the VirtualBoot option isn't yet supported on versions of VirtualBox after 3.2.12. After removing VirtualBox 4.0.2 and installing version 3.1.8, I was able to boot my server from the ShadowProtect Server backup files in about 2 minutes. Granted, I didn't have much data on this server and it was mostly just the OS that was being restored—but I was still impressed.

Licensing

The licensing for ShadowProtect Server is very reasonable. In fact, if you compare competing products I think you'll find that you'd pay more to get all of ShadowProtect Server's features from a competitor. You can purchase individual Windows Server licenses for $995 or Windows Small Business Server (SBS) licenses for $495. If you just need the product for a temporary project, you can purchase the ShadowProtect IT Edition for 2 weeks, 1 month, 3 months, or a year. StorageCraft offers a free 30-day trial, although the trial version doesn't support hardware-independent restore—so you wouldn't be able to use it for a physical to virtual migration.

An All-in-One Solution

In comparing ShadowProtect Server with my own production environment backup routines, I have to admit that I use multiple backup products or scripts; however, ShadowProtect Server's feature set, speed, and ease of use are far superior. I highly recommend this product to anyone in the market for Windows backup software.

InstantDoc ID 129794

ShadowProtect Server

PROS: Extremely flexible; easy to use; provides fast recovery; supports booting from backups or conversion of backup files to a VM; automatically reports on backup job status; backup file management system verifies all backups and consolidates incremental backups into full backup files on a configurable schedule

CONS: No major flaws

RATING: ◆◆◆◆◆

PRICE: $995 for one Windows server; $445 for SBS; volume pricing available

RECOMMENDATION: Anyone in the market for a Windows backup solution should consider ShadowProtect Server.

CONTACT: StorageCraft Technology • 801-545-4700 • www.storagecraft.com

REVIEW

SecureLinx SpiderDuo

An IP KVM device might seem like a luxury, but it can be essential for monitoring mission-critical systems. I recently encountered a Windows server that was intermittently responding to pings during off hours. I tried troubleshooting the server remotely, but the Remote Desktop connection didn't respond. When I connected via IP KVM device, I was able to see the system halting and I could troubleshoot the issue before heading into the office. Accessing systems through an IP KVM device such as Lantronix's SecureLinx SpiderDuo gives you full BIOS-level control of the destination computer. This is helpful when you're trying to view the screen contents of a machine stuck on a startup sequence, change BIOS options remotely, or make configuration changes to a PC via the OS.

SpiderDuo is a unique IP KVM device because of its small size, zero-U rack mounting, expansive configuration options, and optional Internet-accessible service (accessmydevice.com). It supports virtually all versions of Windows, UNIX, Linux, and Mac OS X 10. Figure 1 shows the SecureLinx SpiderDuo.

SecureLinx SpiderDuo setup is a three-step process. You connect the cables, locate the device on the network, and connect through a browser to the destination computer. Using the Quick Start Guide makes cabling setup fast and easy. I attached SpiderDuo's mouse, keyboard, and monitor connections using the supplied female USB connectors and female HD15 monitor connector. Then I connected one USB cable and one monitor output USB cable to the PC. Finally, to set up the device, I connected the attached serial port to a PC and fired up a free terminal emulation program called PuTTY. After configuring the default serial settings per Lantronix's instructions (9,600 bits per second, 8 data bits, no parity, 1 stop bit, and no flow control), I was unable to view the configuration prompts. (I later discovered that the default value for speed was set at 115,200kbps.)

I was disappointed that the configuration prompts weren't viewable, so I switched to plan B and plugged an Ethernet cable connected to the network into the SpiderDuo's Ethernet port. I installed the SecureLinx Spider View utility from the supplied CD-ROM. This enterprise-grade software product lets you manage any number of SpiderDuos. Using the Spider View interface, which automatically found the SpiderDuo, I could open the Java-enabled web-based Spider Manager to access and change the default DHCP settings to a fixed IP address so that I could easily manage the unit on my network. Using this setup method is easier than using the serial port method mentioned in the Quick Start Guide.

Figure 1: SecureLinx SpiderDuo

Access to the SpiderDuo is easy on the local LAN. Simply open a Java-enabled web browser, navigate to the Spider Manager using the IP address of the device, and log on to the device. The web-based Spider Manager has a plethora of useful options, including an exclusive-access feature to limit access to only one user, event logging of user logon activity, authentication via Active Directory (AD) or Remote Authentication Dial-In User Service (RADIUS) servers, and a handy Wake on LAN (WOL) feature for remotely waking up any computer with the requisite BIOS settings. Video performance of the IP KVM device is acceptable, especially when using the automatic configuration mode. However, mouse scrolling is slow, which is a common problem with many IP KVM devices. Compared with Remote Desktop Connection on Windows systems, the mouse performance isn't nearly as responsive.

The optional Internet accessibility feature, accessmydevice.com, is available only on SpiderDuo products purchased directly from Lantronix. This service lets you access the IP KVM console web interfaces through an encrypted web session from any PC, regardless of whether it's on your network. The service is straightforward and easy to use; navigate to accessmydevice.com, enter a supplied user ID and password, and either open the management interface or directly access the computer via the IP KVM device. Select *access my computer* to connect to your internal SpiderDuo IP KVM console web interface, assuming the SpiderDuo IP is connected to a switch port that allows TCP connections to ports 80 and 443. The system works just like you're accessing the SpiderDuo over the internal LAN.

The device has a small footprint for tight spaces, or it can be mounted on the rear of a server rack. Overall, it performs quite well, making it a solid addition to any IT toolkit. SpiderDuo is helpful for troubleshooting systems and for connecting to locked-down computers that don't allow software-based remote access.

InstantDoc ID 129855

SecureLinx SpiderDuo

PROS: Solid device with quality cable connectors; flexible configuration options

CONS: Cumbersome initial setup process; high monthly cost for web-based access

RATING: ◆◆◆◆◇

PRICE: $349 for AccessMyDevice-enabled SpiderDuo from Lantronix; $14.99 to $19.99 monthly, depending on number of devices, for the optional Internet-based AccessMyDevice service; $300 for standard SpiderDuo from online retailers; volume discounts available

RECOMMENDATION: Even if you already own an IP KVM system, you can find a use for SpiderDuo.

CONTACT: Lantronix • 800-526-8766 • www.lantronix.com

Tony Bieda | tonybieda@yahoo.com

MARKET WATCH

Virtualization from the Desktop to the Data Center

Navigate the virtualization technology maze

by Michael Otey

Virtualization has quickly become one of the most widespread technologies in IT today. Despite its near ubiquitous nature, virtualization can be a difficult technology to understand—not because the technology is so complex, but because of the fact that the term *virtualization* is used to describe several different technologies.

When people talk about virtualization, they're typically referring to server virtualization. Server virtualization lets organizations run multiple servers on a single hardware platform. Another closely related form of virtualization is desktop virtualization. Desktop virtualization is used primarily for virtualizing desktop OSs and for creating development and test environments. Another type of virtualization is Virtual Desktop Infrastructure (VDI), which is also called hosted desktop virtualization. VDI uses server virtualization to provide centrally managed desktops throughout an organization. Application virtualization is yet another important type of virtualization. Unlike server and desktop virtualization, in which the hardware platform is virtualized, with application virtualization, the application runs in a virtual or sandboxed environment that isolates the OS from the application.

Microsoft's virtualization information also sometimes includes a technology the company calls Presentation Virtualization—however, I don't consider this to be a real virtualization technology and therefore don't cover it here. For more information about the technology, see the web-exclusive sidebar "Presentation Virtualization: The Virtualization Technology that Isn't," www.windowsitpro.com, InstantDoc ID 129765.

This article will guide you through the maze of today's virtualization technologies. As I step through each of the different types of virtualization, I discuss some of the most significant products that are available, including their position in the market and some of their most important features.

Server Virtualization

Server virtualization is currently one of the hottest trends in IT and is used in several different scenarios, including server consolidation, business continuity, and lab and deployment testing. Server virtualization is accomplished by running virtualization software that lets the server hardware be used by multiple virtual machines (VMs) that are supported on the virtualization layer. Each VM has its own virtual hardware devices and applications and runs its own OS. The supported OSs vary according to the virtualization product. Figure 1 shows an overview of server virtualization.

As you can see in Figure 1, multiple VMs run on top of a shared hardware platform. Today's modern server virtualization products use hypervisor-based virtualization rather than hosted virtualization. This means that the virtualization software runs directly on the system hardware rather than running on the OS. Virtualization software that runs on the OS is typically referred to as hosted virtualization because it requires a host OS. (I explain hosted virtualization in more detail in the following section on desktop virtualization.) Hypervisor-based virtualization provides much lower overhead and significantly better performance than hosted virtualization. Some older server virtualization products can run on older 32-bit x86 servers. However, the newer hypervisor-based server virtualization products require 64-bit x64-based servers. Intel and AMD added features to their processors to let hypervisor-based virtualization function more efficiently. Intel's new technology is called Intel Virtualization Technology (Intel VT); AMD's is AMD Virtualization (AMD-V).

The primary server virtualization products are VMware vSphere 4.1, VMware vSphere Hypervisor, and Microsoft Hyper-V. Other server virtualization products include Citrix's XenSource, Parallels

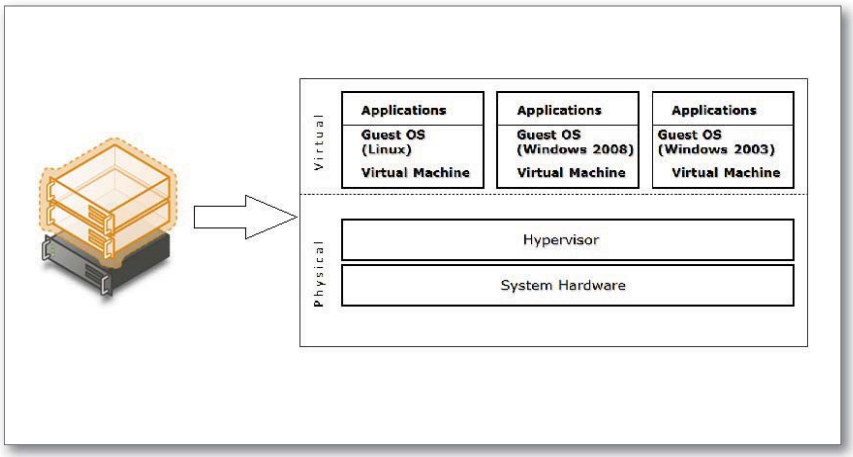


Figure 1: Server virtualization overview

Virtuozzo Containers, and Parallels Server 4 Bare Metal. There are also a couple of legacy server virtualization products: Microsoft Virtual Server 2005 R2 and VMware Virtual Server. Although these products are essentially outdated, they're still available and can be useful in situations in which you need to support virtualization on 32-bit hosts.

VMware vSphere 4.1 and VMware vSphere Hypervisor (ESXi). Without a doubt, VMware vSphere is today's premier server virtualization platform. VMware first released ESX Server in 2001, and the product quickly established itself as the leader in the enterprise virtualization space (despite Hyper-V's progress in the server virtualization space). IDC conservatively estimates that VMware had 50 percent of the server virtualization market in 2010. VMware offers two hypervisor server products: VMware vSphere 4.21 (ESX Server) and a free version called VMware vSphere Hypervisor (formerly named ESXi).

VMware vSphere supports several enterprise-oriented features. For example, it supports almost all Windows and Linux versions as guest OSs. It also supports VMs with up to 255GB of RAM and four-way virtual SMP, as well as the capability to hot-add CPUs and RAM in the VMs. VMware ESX Server also provides a couple of important availability features: VMware VMotion and VMware Storage VMotion. VMotion lets running VMs move between active ESX Server systems. Similarly, Storage VMotion lets you move a VM's virtual hard disk files to a new storage location with no downtime for the VM's end users. VMware ESX Server has included both these features for several years, so they're quite mature. Unlike Hyper-V's live migration, a single ESX Server system can run VMotion on several different hosts simultaneously.

The VMware vSphere hypervisor is architected differently than Hyper-V. The primary difference is that VMware's hypervisor includes the device drivers as part of the hypervisor. This results in somewhat better performance and reliability, but it also limits the hardware platforms that are supported. VMware vSphere is a more expensive virtualization platform than Hyper-V because unlike with Hyper-V, you must license vSphere separately from the Windows Server OS. However, vSphere can still benefit from Microsoft's virtualization licensing features. For instance, if you run Windows Server 2008 R2 Datacenter Edition on VMware vSphere, the Datacenter license covers all the virtual Windows Server instances on the vSphere server. Windows Server virtualization licensing covers all virtualization products, such as VMware vSphere, that are part of Microsoft's Windows Server Virtualization Validation Program. You can learn more about the Windows Server Virtualization Validation Program at www.windowsservercatalog.com/svvp.aspx. You can download a trial version of VMware ESX Server 4.1 from www.vmware.com/tryvmware/index.php?p=vmware-vsphere&lp=1. You can download VMware's free ESXi from www.vmware.com/products/vsphere-hypervisor/index.html.

Hyper-V and Hyper-V Server 2008 R2. Hyper-V, Microsoft's server virtualization solution, is the primary competitor to VMware vSphere. Microsoft first released Hyper-V in 2008 and later updated it with the release of Server 2008 R2. Hyper-V is the runner-up in the virtualization race. IDC estimates for 2010 show Microsoft with about 26 percent of the virtualization market; that growth for Hyper-V was an impressive 215 percent (albeit from a lower starting point). Hyper-V is delivered in two ways: as a Server 2008 R2 and Server 2008 role, or as the free Hyper-V Server 2008 R2 product.

Hyper-V was originally released with Server 2008. This initial release became known as Hyper-V 1.0. The Hyper-V 1.0 release didn't support live migration. Instead, it supported quick migration, a technology that incurred some downtime as VM files were transferred between cluster nodes. Microsoft updated Hyper-V with the release of Server 2008 R2; this release is known as Hyper-V 2.0. Hyper-V 2.0 supports live migration, which lets VMs move between different Hyper-V hosts with no downtime. Live migration is essentially the Microsoft counterpart to VMware VMotion. Hyper-V 2.0 also provides support for VMs with up to four-way virtual SMP and up to 64GB of RAM per VM.

The Hyper-V role in Server 2008 R2 and Hyper-V Server 2008 R2 are based on the same technology, which is quite different from VMware's design. Hyper-V uses a hypervisor, but the drivers come from the parent partition rather than the hypervisor. (For information about the differences in VMware's hypervisor and Microsoft's hypervisor, see "Virtualization Shootout, Part 1," InstantDoc ID 98879; "Virtualization Shootout, Part 2," July 2008, InstantDoc ID 99248; and "Virtualization Rematch," December 2008, InstantDoc ID 100573.)

Numerous differences exist between Hyper-V Server 2008 R2 and the Hyper-V role in Windows Server. One of the main technological differences is the fact that Hyper-V Server 2008 R2 and Hyper-V Server 2008 must be managed remotely; there's no local GUI. Another important difference is licensing. Hyper-V Server 2008 R2 and Hyper-V Server 2008 include no licenses for any host or guest OSs. With Server 2008 R2 and Server 2008, you get at least one license for running Server 2008 and additional licenses depending on the edition you have. Server 2008 Standard Edition provides an additional license for one

active instance of Windows Server running on a VM. Server 2008 Enterprise Edition licensing covers four active Windows Server instances running on VMs. Server 2008 Datacenter Edition provides for running an unlimited number of active Windows Server instances with no additional licensing costs. You can learn more about Server 2008 and virtualization at www.microsoft.com/windowsserver2008/en/us/hyperv-main.aspx. For more information about Windows Server licensing and virtualization, go to download.microsoft.com/download/e/e/c/eecf5d44-9a88-43d8-afdb-d2ab82be035c/R2_License_Guide-ONLINE.pdf. You can download the free Hyper-V Server 2008 R2 at www.microsoft.com/hyper-v-server/en/us/default.aspx.

Other server virtualization products. Although Hyper-V and VMware ESX Server comprise the vast majority of today's server virtualization market, they aren't the only players in the space. Citrix, the company that's probably best known for its Terminal Services product, offers XenServer. XenServer is based on the open-source Xen hypervisor. Citrix acquired XenSource in 2007. Like Hyper-V, the XenServer architecture uses a primary partition. Unlike Hyper-V, XenSource is a Linux-based virtualization product. XenSource supports hardware-assisted virtualization. It also supports moving VMs between hosts with no downtime via a technology called XenMotion. There are several editions of XenServer. You can download a free version of XenServer from www.citrix.com/English/ps2/products/feature.asp?contentID=2300356.

Another company in the server virtualization market is Parallels. This company is probably best known for its Mac desktop virtualization product (Parallels Desktop for Mac). Parallels has two products in the Windows server virtualization space: Parallels Virtuozzo Containers and Parallels Server 4 Bare Metal. Virtuozzo began as a Linux product that made its way to Windows. It's primarily used by hosting providers. Parallels Virtuozzo Containers is a different type of virtualization product. Rather than virtualizing at the hardware level the way ESX Server and Hyper-V do, Virtuozzo Containers virtualizes at the OS level. This method has less overhead than hardware virtualization does but also less flexibility because all the virtual containers must have the same OS. Parallels Server 4 Bare Metal is a hypervisor-based virtualization platform that allows up to 12 virtual CPUs per VM and supports up to 64GB of RAM per VM. Notably, Parallels Server 4 Bare Metal also provides USB support in its VM, which neither vSphere nor Hyper-V do. You can learn more about Parallels server virtualization products at www.parallels.com/virtualization/server.

Desktop Virtualization

Hardware virtualization such as server and desktop virtualization were really born in VMware Workstation, which was first released back in 1998. Desktop virtualization is primarily used for development and test environments. Like server virtualization, desktop virtualization lets you run multiple VMs on a single hardware platform. Again, each VM thinks it's running on its own hardware and each has its own OS and applications. Unlike server virtualization, which is hypervisor-based, desktop virtualization uses hosted virtualization. Figure 2 shows an overview of how desktop virtualization works.

The desktop virtualization architecture has a hardware layer at the bottom; the host's desktop OS runs on top of that layer. The virtualization software is installed on the host's OS. This setup doesn't provide the same level of performance as hypervisor-based virtualization, but it can provide better usability and a greater range of features. For example, desktop virtualization products almost all provide access to the host's USB drives, support for audio, and integration with the desktop system's power management features such as sleep and hibernate. Some desktop virtualization products offer support for 3D graphics and DirectX. These features aren't available in most hypervisor-based server virtualization products.

The primary PC desktop virtualization products are VMware Workstation 7.0, VMware Player 3.0, Microsoft Virtual PC 2007, Microsoft Windows Virtual PC, Windows 7's Windows XP Mode, Oracle's VirtualBox, and Parallels Desktop 4 for Windows. In addition to these products, there are a couple of Mac desktop virtualization products: VMware Fusion and Parallels Desktop for Mac.

VMware Workstation 7.0. VMware Workstation was the original x86 virtualization program, and it certainly hasn't stood still. VMware Workstation 7.0 is the clear leader in the desktop virtualization market. As you might expect for a mature product, Workstation 7.0 runs on both Windows and Linux and supports almost all Windows and Linux versions as VM guest OSs. It also supports Intel VT and AMD-V hardware-assisted virtualization. Workstation 7.0 supports several advanced features that aren't found in other products. For example, Workstation supports the Windows 7 Aero interface, 3D graphics, and DirectX 9.0 in VMs. Workstation also supports up to eight virtual processors, the ability to capture and replay user actions in the virtualization session, and VM file encryption. VMware Workstation 7.0 costs $189; you can download a trial version from www.vmware.com/tryvmware/?p=vmware-workstation&lp=1.

VMware Player 3.0. VMware Player 3.0 is a free desktop virtualization offering from

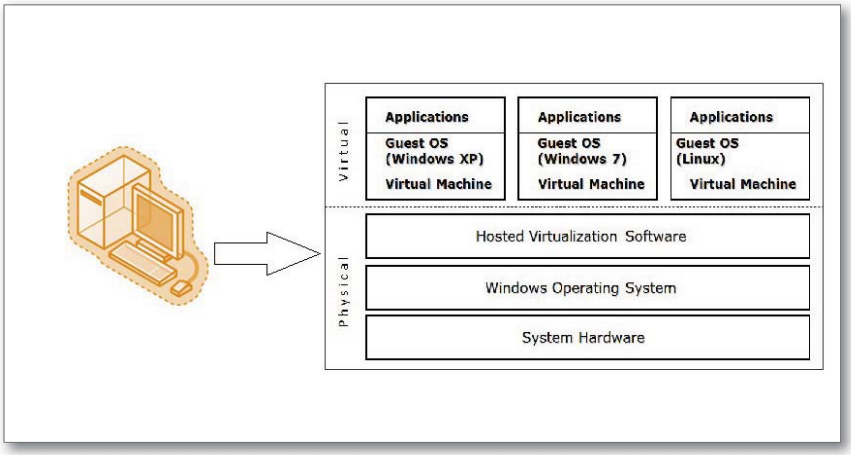


Figure 2: Desktop virtualization overview

VMware. As its name implies, the original version of Player was only able to run (or play) existing VMs. However, VMware later updated the Player product with the ability to create VMs. As a free product, Player is basic virtualization software that lacks most of the advanced features found in Workstation. However, it has the same wide array of host and guest support. You can download VMware Player 3.0 from downloads.vmware.com/d/info/desktop_downloads/vmware_player/3_0.

Virtual PC 2007. Microsoft was a latecomer to the virtualization market. The company's initial offering in the virtualization space was Virtual PC 2004, which Microsoft acquired from Connectix in 2003. At first Virtual PC 2004 was a paid product, but with the release of Virtual PC 2007 the product became free. Both 32-bit and 64-bit versions of Virtual PC are available. The product can run on Windows 7 and older Windows XP OSs. It can't run on Linux; although you can make Linux run as a guest, this configuration has never been supported. Virtual PC 2007 is still available for download, but it's essentially a legacy product. Microsoft ceased development of the product to focus on its successor, Windows Virtual PC. You can find Virtual PC 2007 at www.microsoft.com/downloads/en/details.aspx?FamilyID=04d26402-3199-48a3-afa2-2dc0b40a73b6.

Windows Virtual PC and Windows XP Mode. Windows Virtual PC runs only on Windows 7. It adds several missing features to what Virtual PC 2007 offers, including support for USB drives. It supports Intel VT and AMD-V hardware-assisted virtualization but doesn't require it. Although it's an improvement over Virtual PC 2007, Windows Virtual PC isn't in the same class as VMware Workstation. It doesn't support running Linux as a guest, nor does it officially support Windows Server OSs as a guest—although both can be made to work.

Another closely related desktop virtualization technology that you might have heard of is Windows 7's Windows XP Mode. Windows XP Mode is built on top of Windows Virtual PC and is designed to let you seamlessly run Windows XP programs from the Windows 7 desktop. Its main purpose is to support legacy applications on Windows 7. Windows XP Mode uses Windows Virtual PC to launch a VM in the background, then surfaces applications running on a VM that uses a guest Windows XP OS on your Windows 7 desktop. You can download Windows Virtual PC and Windows XP Mode from www.microsoft.com/windows/virtual-pc/download.aspx.

Microsoft also offers another version of this type of desktop virtualization technology, called Microsoft Enterprise Desktop Virtualization (MED-V). Like in Windows XP Mode, legacy application compatibility is the main purpose behind MED-V. MED-V lets applications that are running on a VM be seamlessly integrated with the user's desktop. Unlike Windows XP Mode, MED-V is built on top of Microsoft's Virtual PC product. MED-V is part of the Microsoft Desktop Optimization Pack (MDOP), which is available only to Software Assurance customers. You can learn more about MED-V at www.microsoft.com/windows/enterprise/products/mdop/med-v.aspx.

Other desktop virtualization products. In addition to the VMware and Microsoft desktop virtualization products, there are a handful of other desktop virtualization products available. The other Windows desktop virtualization products are Oracle's VirtualBox and Parallels Desktop 4 for Windows & Linux. VirtualBox is an open-source virtualization product that was formerly a part of Sun Microsystems's product line but was acquired by Oracle in January 2010. VirtualBox is a free product that supports the widest variety of host OSs of any desktop virtualization product. VirtualBox has host support for Windows 7, Windows Vista, XP, Linux, Mac OS X, Solaris, Open Solaris, and FreeBSD. It offers support for Intel VT and AMD-V, as well as 32-bit and 64-bit guest OSs. You can find VirtualBox at www.virtualbox.org. Parallels Desktop 4 for Windows & Linux is a commercial desktop virtualization product. It supports Intel VT and AMD-V and runs VMs that can have up to eight virtual CPUs and 8GB of RAM. Parallels Desktop 4 for Windows & Linux can run on 32-bit and 64-bit versions of Windows 7, Vista, XP, Debian 5.0, Fedora 11, Mandriva 2009, openSUSE 11.1, Red Hat Enterprise Linux (RHEL) 5.3, SUSE Linux Enterprise Server (SLES) 11, and Ubuntu 9.04. Parallels Desktop 4 for Windows & Linux costs $79.99; you can find it at www.parallels.com/products/desktop/pd4wl.

In addition to these Windows-based desktop virtualization products, there are also a couple of virtualization products for the Mac. The main use for these Mac virtualization products is to let you run various versions of Windows, including Windows 7, on the Mac desktop. Notably, there's no virtualization product that officially supports running Mac OS X in a PC-based host. The two main Mac desktop virtualization products are Parallels Desktop 6 for Mac and VMware Fusion 3. Parallels Desktop 6 for Mac is the leader in the Mac desktop virtualization market; it supports the Windows 7 Aero UI and 3D graphics. Parallels Desktop 6 for Mac costs $79.99; you can find it at www.parallels.com/products/desktop. VMware Fusion is the other notable product in the Mac desktop virtualization market; its VMs support the Windows 7 Aero interface and 3D graphics. VMware Fusion costs $49.99; you can find it at www.vmware.com/products/fusion.

Virtual Desktop Infrastructure

Another virtualization technology that's gaining popularity in the enterprise and large business markets is VDI, or hosted desktop virtualization as it's sometimes called. Although its name makes it easy to confuse with desktop virtualization, VDI isn't really desktop virtualization at all. Instead, it's a technology that enables centralized management of client systems. Figure 3 shows an overview of how VDI virtualization works.

With VDI, the virtualization software doesn't run on the desktop at all. Instead, a virtualization server platform such as Hyper-V or ESX Server runs many VMs; each VM is built using a client OS such as Windows 7 or XP. Client systems run a form of receiver software that uses a remote desktop type of protocol such as RDP or ICA to connect to the client VM that's running on the server virtualization platform. Typically, another system called a connection broker sits between the client systems and the virtualization server. The connection broker identifies the incoming connections and directs them to the appropriate VM.

As you might imagine, because this scenario is running all of the client systems as VMs, it requires large amounts of bandwidth and computing power for the

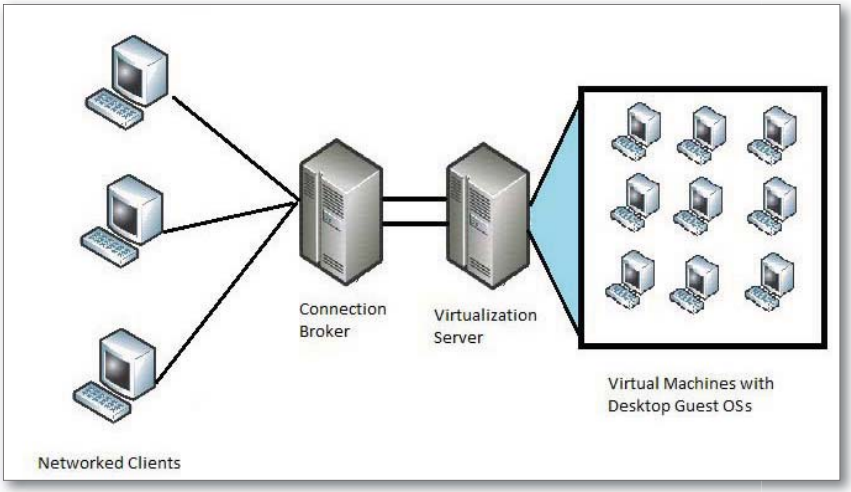


Figure 3: VDI overview

virtualization host. However, the clients require very few resources and can even be thin clients or mobile devices. In addition, because all the client resources are centralized, IT has much more control over the client systems.

There are two main types of VDI approaches. One approach uses prebuilt client images; the other approach dynamically builds the client system using a shared "golden" OS image and dynamically combines this image with personalized user settings, applications, and data. This dynamic approach can use dramatically less storage than individual images. For more information about VDI, you can refer to John Savill's VDI series ("Virtual Desktop Infrastructure, Part 1," January 2011, InstantDoc ID 129007, and "Virtual Desktop Infrastructure, Part 2," April 2011, InstantDoc ID 129572). There are four main players in today's hosted desktop virtualization space: the Microsoft VDI Suite, Citrix's XenDesktop, VMware View, and Quest's vWorkspace.

Microsoft VDI Suite. The Microsoft VDI Suite is really something of a misnomer. The name implies that it's a product, but it's really a bundling of several different Microsoft virtualization technologies, including Hyper-V, Microsoft System Center Virtual Machine Manager (VMM) for managing the desktop VMs, Microsoft System Center Operations Manager for monitoring hosts and VMs, Microsoft System Center Configuration Manager (SCCM) for creating desktop images, and Windows Server's Remote Desktop Services (RDS) with its Remote Desktop Session Broker and Remote Desktop Gateway. Microsoft markets two versions of this product: the Microsoft VDI Standard Suite and the Microsoft VDI Premium Suite. The main difference is that the Premium Suite includes Microsoft Application Virtualization (App-V), in addition to the other products that comprise the Standard Suite. None of these products are specifically intended for VDI. However, they can each play a different role in making VDI work. The suites are simply a way to help customers handle the licensing complexities of this mishmash of different technologies. Most customers who want to use VDI with Hyper-V gravitate to the next product I discuss: Citrix's XenDesktop.

XenDesktop. XenDesktop offers a simpler and better VDI solution for Hyper-V than Microsoft's own technologies, mainly because it's specifically designed to address VDI. XenDesktop can deliver VDI services to all types of devices using its FlexCast technology. As you might guess, clients connect to the server using Citrix's ICA protocol. In addition, XenDesktop lets you manage all VDI services from a single console. Citrix offers way too many editions of XenDesktop to make any product decision easy. It offers a free Express version, as well as Standard, Advanced, Enterprise, and Platinum versions. The Platinum edition includes Citrix's high-performance HDX technology for 3D graphics. You can learn more about the XenDesktop editions at support.citrix.com/proddocs/index.jsp?topic=/xendesktop-snma/cds-overview-editions-overview-wrapper.html, and you can download the Express version from www.citrix.com/lang/English/lp/lp_1859991.asp.

VMware View. Not to be left out of any part of the virtualization market, VMware provides its own VDI solution with VMware View. VMware View 4.5 uses VMware's own PCoIP protocol to communicate with client devices, and the VMware View Client supports a local mode that lets you use VDI services without an active connection to the virtualization server. VMware offers two editions of View: VMware View Enterprise and VMware View Premier. The Premier edition includes the View Client with the local mode, as well as the application virtualization product VMware ThinApp. You can learn more about VMware View 4.5 at www.vmware.com/products/view; you can download a 60-day trial from www.vmware.com/tryvmware/?p=view45&lp=1&rlz=1I7GGIE_en&ie=UTF-8&oe=UTF-8&sourceid=ie7.

vWorkspace. A lesser-known player in the hosted desktop virtualization market, Quest's vWorkspace 7.2 has actually been in the VDI space for several years. vWorkspace works with Hyper-V, VMware vSphere, and Parallels Virtuozzo. vWorkspace offers a wizard-driven setup, as well as an integrated PowerShell management framework. Quest also offers the Experience Optimized Protocol (EOP), which enhances RDP support for screen updates and images. You can learn more about vWorkspace at www.quest.com/vworkspace. You can register for a trial download of vWorkspace at www.quest.com/common/default.aspx?backtourl=/common/registration.aspx?requestdefid=28560.

Application Virtualization

Although server and desktop virtualization are the technologies that you usually think of when you refer to virtualization, application virtualization is another emerging type of virtualization technology. Server and desktop virtualization work at the hardware level, whereas application virtualization works at the application level. Hardware virtualization and application virtualization solve very different problems. Server virtualization addresses server deployment, consolidation, management, and availability. Application virtualization addresses application deployment, isolation, and management.

With application virtualization, software running on the client system provides support for virtual applications. The client virtualization layer provides the virtual application with a copy of the system's file system, registry, and other system I/O points. When the virtual application runs, it interacts with the virtual system environment and doesn't modify the true underlying host system's physical registry and file system. Application virtualization allows multiple applications that might normally conflict with one another to run together on the same system with no conflicts because each application runs in its own virtual environment. Likewise, because each virtual application runs in its own space, DLL hell is eliminated, in which installing one application can write over the DLLs used by another application. The two primary application virtualization products are Microsoft App-V and VMware ThinApp. Figure 4 shows an overview of application virtualization.

App-V. App-V is Microsoft's application virtualization platform. Microsoft acquired the technology for App-V by purchasing Softricity's SoftGrid product in 2006. The biggest advantage of App-V is probably its no-touch application deployment. App-V is integrated with Active Directory (AD). Administrators can assign virtual applications to users and groups, then those applications can be streamed to end users' systems without any manual intervention.

With App-V, the applications that are virtualized are run through a process called the Microsoft Application Virtualization Sequencer, which breaks the application into pieces that can be streamed to the users' desktops. The virtual applications are stored on System Center Application Virtualization Management Server, which not only stores the virtual applications but is also responsible for streaming them to the users' desktops where they are executed by the virtualization client software.

One benefit of the sequencing process is that only the parts of the application that are used are streamed to the users' desktops. For example, when you run an application such as Microsoft Office—which typically requires several hundred megabytes—through the sequencer, the sequencer breaks that application into many smaller sections that can be individually streamed to the client. The end result is that when the client initially uses the application, it doesn't need to wait for hundreds of megabytes to be streamed to the system before the app can be used. Instead, only the code necessary to run the executable part of the application being requested will be streamed to the client. This might be only a few megabytes, yet the application will execute normally in the virtual client environment. Later, as the end user requests additional functions and features, just the code necessary to execute those features will be streamed to the client. App-V is part of MDOP, which is available only to Software Assurance customers. You can learn more about App-V at www.microsoft.com/systemcenter/appv/default.mspx.

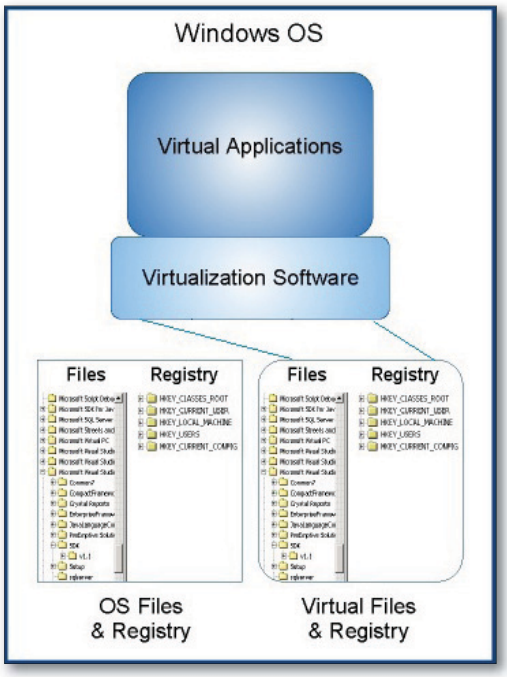


Figure 4: Application virtualization overview

VMware ThinApp. VMware ThinApp was originally acquired from a company called ThinStall back in 2008. ThinApp works very differently from App-V. It's simpler and has fewer infrastructure requirements. ThinApp application virtualization doesn't require a client to be installed on the target system. Instead, the virtualization client is prepackaged with the application into a single executable file that can be distributed to the target systems and run immediately. This bundling lets you easily deploy virtualized ThinApp applications on USB drives or from network shares. After the virtual application executable file is copied to the target system, you can run the virtual application just like any standard executable program.

VMware ThinApp provides a Virtual Operating System (VOS) layer that encapsulates the application code, letting applications run on a host OS with no modifications to that OS. The VOS is very lightweight, taking less than 300Kb of disk space and 1MB of RAM to run. The VOS provides a virtual registry layer and a virtual file system layer, and it handles loading the executable and any required DLLs. When you run the virtual applications, the VOS is loaded, which in turn loads the application into its virtual environment. The VOS supports all the OS processing necessary to run Windows applications, including out-of-process COM calls, services-based COM calls, manifest policy processing, and side-by-side DLL resolution. You can learn more about VMware ThinApp and download a 30-day trial from www.vmware.com/products/thinapp. VMware also offers a free starter edition of this product with the purchase of VMware Workstation 7.0.

Living in the Virtual World

Virtualization has become a staple in today's IT infrastructure. Server virtualization is used for server consolidation and business continuity scenarios. Desktop virtualization is primarily used for testing and development. Hosted desktop virtualization is used for centralized desktop management. Application virtualization is used for centralized application deployment and improved application compatibility. Understanding today's virtualization marketplace will help you select the appropriate type of virtualization technology for your business's needs.

InstantDoc ID 129722

Michael Otey
(motey@windowsitpro.com) is technical director for *Windows IT Pro* and *SQL Server Magazine* and author of *Microsoft SQL Server 2008 New Features* (Osborne/McGraw-Hill).

Exchange Server Auditing Software

It's the software that watches the watchers—and everyone, and everything, else

by B. K. Winstead

Why should you perform auditing on your Microsoft Exchange Server environment? If you're asking yourself that question, chances are you're in trouble already, even if you don't know it. Even without legal or regulatory requirements, there are probably many good reasons you want to keep a close watch on your Exchange systems, from general security to performance. Knowing what to look for and where to find it—that's where things get a little trickier.

Exchange Server 2010 introduced tools to perform administrator auditing, although if you're not a PowerShell aficionado, you're probably not going to like them. In "Auditing Administrators' Actions with Exchange 2010" (InstantDoc ID 129720), Tony Redmond walks you through enabling the new native tools, shows you how to used the cmdlets to search and export data, and describes the few out-of-the-box reports you have available. Exchange 2010 has the ability to find whatever you might need, but there's no fancy GUI—at least, not up to this point.

Third-party vendors, as usual, can probably fill your auditing needs quite nicely—and provide you with an administrative GUI to get the job done. In the accompanying buyer's guide table, you can see a comparison of features of the products in this market space. But first, let's examine some of the factors driving the need for Exchange auditing, and then take a look at what you should expect to find in a third-party product.

The Need for Auditing

In certain industries—medical, financial services—strict legal requirements govern how data is handled and who has access to it. And for that, we're all quite thankful—when it works. We've all heard of regulations such as HIPAA or standards such as PCI. If you manage an Exchange organization where such regulations are enforced, clearly you're familiar with auditing. But no organization can really afford to ignore it. As Tom Crane, product manager for Quest Software, said, "I don't think any industry out there is free and clear for not having auditing."

Even if you adhere to certain regulations, it's sometimes unclear what exactly they mean or how to monitor for them. In some cases, companies might not even be sure which regulations apply to them. Certainly that was the case when HIPAA and Sarbanes-Oxley and such first appeared, but as Crane said, "As time goes on, the definitions of what needs to be done have started to mature." He also noted that both auditors and companies have come to a better understanding of the data and what's required of them by these regulations.

But let's face it: There's a lot of data. A lot of potentially regulated information can pass through or reside in an Exchange organization. Wendy Yale, senior director of marketing for Varonis Systems, spoke to this point. "Email nowadays is the cornerstone of collaboration," Yale said. "It's even more important today than traditional communication methods—people just don't talk on the phone as much. It's the heart of collaboration, and because of that, the data is growing so, so fast. If you look at most companies, it's not even [that they're] not keeping up with it; in the worst cases, it's not even approaching coming to a manageable ratio."

In most cases, systems have grown organically over time. As email and other electronic communication methods have gained prevalence, all that data just keeps piling up, and your needs for things such as auditing probably weren't thought of at the beginning. As Yale points out, "It's hard to go back and fix it once something's started." So, having the right tools that can sift the data and provide it to you in a useful form is a must.

Although the drive to find an auditing solution might come from Exchange administrators themselves, it's just as possible that it might be a suggestion—or demand—from higher up the chain of command in a business. As Crane said, "A lot of times, it comes down to board members, CEOs—those are the big drivers, all the executives. They're really particular about a lot of intellectual property, a lot of confidential information getting passed back and forth. Exchange administrators have access to backup accounts, or other accounts that have the natural, delegated permissions. So [executives] want to keep tabs if someone is using those [accounts] inappropriately."

No Exchange admin wants to feel like someone's watching over their shoulder all the time, but this is a reality of the corporate world. And Crane's point is valid: Admins are the ones who have access. Furthermore, auditing isn't just about watching for violations or unauthorized access; it can also be used to find problems when a change goes awry. Who made that change, and why? What was it supposed to be? A good auditing solution will help you spot such problems.

What Should You Audit?

The question of what specifically in your environment to look at is going to be answered differently for different organizations, and quite possibly answered differently at different times. In speaking with the four companies providing auditing products for Exchange, I found that they all had valuable advice, and all slightly different. Not surprising, this advice more or less aligns with the strengths of their particular products.

According to Michael Fimin, president and CEO of NetWrix, it's important to track all changes in your Exchange environment. "Every time you change something, it has to be audited," Fimin said, "especially if there's more than one person involved in Exchange management. It has to be tracked. And everybody has to be aware of what's going on, what things are being changed, what permissions are being changed, what mailboxes change, whatever." NetWrix Exchange Change Reporter is part of the company's Change Reporter Suite, which has modules to monitor your entire IT infrastructure, including Active Directory (AD), SharePoint, SQL Server, and much more.

Fimin was able to break down into three categories what he feels an auditing solution should be able to do for you. "First of all, it's the archiving of changes. You have to be able to track the history," he said. "If your auditors come in and say, 'Show me what changed 5 years ago,' you have to be able to do that." Fimin noted that in certain industries, you might need to be able to audit changes back as far as 7 years.

His second requirement is the ability to effectively report on the data you collect. "You have to be able to create reports for specific types of changes, or just for any changes from a certain criteria," he said. "And the alerting capability would be a third important piece of the puzzle. You have to be able to create alerts on certain sensitive types of events, such as those that can affect security and compliance."

For Adam Laub, vice president of marketing for STEALTHbits, and Barbara Baumle, technical product manager for messaging and mobility at the company, some of the important auditing features Exchange administrators need center around access control. "Not just looking at access activity," Laub said, "but actually who has access, and who has access over time, so that they can keep track of critical changes to mailbox rights and permissions, make sure that you don't have high-risk mailboxes sitting out there where accounts like Default and Anonymous are open for any user to essentially log on to that mailbox and be able to peruse through it."

The STEALTHbits product, StealthAUDIT Management Platform for Exchange, is also part of a larger auditing platform from the company, a good point to keep in mind if your auditing interests stretch beyond Exchange itself. As far as what customers are looking to keep an eye on, Baumle said, "We find it's very specific per corporation,

Company	Product	Price	Exchange Versions Supported	Run On What OSs?	Other Software Dependencies for the Product?	Minimum Hardware Requirements?	Integrates with Larger Suite of Auditing Solutions the Company Offers? If So, Does This Product Also Stand Alone?	Other Vendors' Solutions that the Product Integrates with	Is Auditing Based on Native Exchange Logs or Another Method?
NetWrix 888-638-9749 201-490-8840 www.netwrix.com	NetWrix Exchange Change Reporter	Per enabled AD user, starting from $5.25 per user (for 150 users) to $0.40 per user (for 100,000 users)	2010/2007/2003	Windows 7/Vista/XP; Windows Server 2008 R2/Server 2008/2003	.NET Framework 2.0, SQL Server Express 2005 or later (optional)	2.4GHz CPU, 2GB RAM, 100GB available disk	Part of NetWrix Change Reporter Suite, and also stands alone	Microsoft System Center, ArcSight, and others	Combined approach (native logs, configuration data, agents), all configurable
Quest Software 800-306-9329 949-754-8000 www.quest.com	Quest Change-Auditor for Exchange	North American pricing begins at $12 per managed mailbox	2010/2007/2003	Windows 7/Vista/XP; Server 2008 R2/2008/2003 R2/2003	.NET Framework 3.5 SP1 or higher; Microsoft Data Access Components 2.8 SP1; Microsoft XML Parser 6.0; Microsoft SQLXML 4.0	2 2GHz CPUs; 4GB RAM; others	Integrates with other Quest Software products, and also stands alone	Microsoft System Center; software development kit available to provide integration with other solutions	Based on patent-pending technology
STEALTHbits Technologies 201-447-9300 www.stealthbits.com	StealthAUDIT Management Platform for Exchange	Priced per mailbox	2010/2007/2003/2000	Server 2008/2003	SQL Server 2005 or later (Express, Standard, or Enterprise Editions)	Dual core or multiple CPU; 2GB–4GB RAM; 30GB available disk	Part of the StealthAUDIT Management Platform (SMP), and also stands alone	Extracts data from ODBC-compliant data sources for reporting; writes notification events to the Windows event log for monitoring solutions such as System Center Operations Manager to alert upon	Leverages multiple data collection mechanisms, protocols, and APIs to communicate with and extract data from a wide variety of data sources
Varonis Systems 877-292-8767 www.varonis.com	Varonis DatAdvantage for Exchange	Starts at $8,000	2010/2007 (SP2 and SP3)/2003 (planned for 2011)	Server 2008/2003 R2 SP2/2003 SP1	SQL Server 2005 Standard or Enterprise with Reporting Services with SP2 or SP3 or SQL Server 2008 Standard or Enterprise	VMware or single server with dual CPU or HT/dual core (2GHz and above); 2GB RAM; 60GB available disk	Part of Varonis Data Governance Suite, and also stand alone	No	Leverages a lightweight agent that provides far more event types, with less server overhead, than native Exchange auditing

depending on what they actually want to see and what's important to them." So either find a solution that offers the greatest amount of choice in how to search and audit and report, or figure out exactly what you're going to need ahead of time.

Like Fimin, Quest Software's Crane had three basic capabilities he thought any auditing product should have. First, you should expect the product to provide ongoing analysis of your overall environment. You should also expect it to help you maintain compliance within your organization by auditing for violations. And third, the product should provide real-time alerts on policy violations.

Even more specifically, Crane talked about the type of information you should be capturing for any change. "It sets out to answer the six Ws," he said. "Who made the change? When did it happen? What object was changed? What system captured it, or what Exchange server did it come from? Where did it originate? Why did it happen?" In addition, the product should capture before and after values for changes, whenever appropriate—and maintain that data.

For Varonis, a key point is the problem of data ownership. You've got public folders in your environment, but it's not always simple to tell who they belong to or who is actually using them. Varonis DatAdvantage for Exchange, which is focused on data governance, can provide this information as well as make recommendations about who has permissions that they shouldn't. As Yale said, "That's powerful, when you provide context to people in addition to just giving them visibility about what exists, because it gives them the intelligence to make proactive decisions about how to move forward." And really, isn't that the real idea behind all this auditing in the first place?

All the Basics

When I began researching Exchange auditing products, I was surprised to find so few companies offering such solutions—only four, each of which spoke with me about their offerings. The good news, if you're in the market, is that means there are fewer products to wade through. Each of the four products performs all the basics of auditing, reporting, and alerting that you would expect, yet each one comes at if from a little different angle, or focuses in a slightly different way. Note that this is a buyer's guide, not a review, so further investigation of the products before purchase is warranted. Check out the feature comparison table, then visit the vendors' websites. Some of the products have trial versions or freeware versions, so you can get a solid understanding before committing to a full deployment. Good luck!

InstantDoc ID 129991

B. K. WINSTEAD
(bwinstead@windowsitpro.com) is a senior associate editor for *Windows IT Pro*, *SQL Server Magazine*, and *SharePoint Pro*, specializing in Exchange Server, messaging, mobility, and unified communications.

	Tracks Changes to Permissions?	Changes to Configurations?	End User Actions?	Administrator Actions?	Non-Owner Mailbox Access?	Provides Time of Change?	Provides Location from Which Change Was Made?	Provides Both Before & After Values?	Provides Preconfigured Reports? (Approximate Number)	Provides Ability to Create Custom Reports?	Preconfigured or Customizable Alerting?	Alerting Provided by?	Features that Either Help Fix or Roll Back Changes
	Yes	Yes	Yes	Yes	Yes (via add-on module)	Yes	Yes	Yes	Yes (30)	Yes	Both	Email, SMS	Rollback Wizard
	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes (40)	Yes	Both	SMTP, SNMP, WMI	N/A
	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes (300–400)	Yes	Customizable	Email, Windows event logs, command-line processes	SMP Action Module Framework
	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes (49)	Yes	Both	Email	Includes sandbox to simulate permission changes, and the ability to roll back permissions changes

INSIGHTS FROM THE INDUSTRY

Top Security Trends for 2011

I attended the RSA Security conference in late February and came away with an enhanced appreciation for what IT managers, CIOs, and CISOs face on a daily basis. Any IT security strategy is all about risk mitigation, the process of implementing the most effective security possible with the finite resources at your disposal.

The security market seems to have rebounded significantly from last year's rather anemic RSA, with Comodo Founder and CEO Melih Abdulhayoglu telling me that "RSA this year was great. People had budgets [for purchasing security products and services] this year, which was a big contrast with last year's RSA."

Mobile devices. Android-based devices seemed to be getting the most attention, partly from having the largest smartphone market share and from news concerning recent (and high-profile) security incidents involving Android devices.

"There is a need for better mobile device security, but people aren't shouting from the rooftops yet," Abdulhayoglu told me. Abdulhayoglu also seconded the idea that Android devices were leading candidates for security solutions. Meanwhile, Apple's iPhone seems to benefit—from a security standpoint—by having a comparatively closed development environment.

Cloud federation and security. While some progress has been made toward improving cloud security, many security obstacles remain. Lieberman Software President and CEO Philip Lieberman echoed that sentiment, saying that, "Customers have a real reason to be concerned. There's a lack of transparency and consistency when it comes to logs and auditing, to reveal what is truly happening in a cloud environment."

I spoke with a number of other vendors who were trying to address cloud security and federation issues with new products and services, such as Credant Technologies' new cloud-based security platform, designed to help enterprises address some security concerns about cloud computing by encrypting data in private clouds. RSA unveiled a new cloud-based federation service called the RSA Cloud Trust Authority, while Verizon rolled out a new enterprise identity service. Qualys updated many of its cloud-based security solutions, including updates to QualysGuard Policy Compliance and QualysGuard Web Application Scanning (WAS).

Security social media. Many experts are cautioning IT and HR departments to back off from more draconian responses to social media use in the workplace, which can range from banning use of Facebook and Twitter to limiting access to those services to a limited number of PCs. Ben Rothke, a senior security consultant at BT Global Services, believes that organizations have to "get in front of the social media wave" and be more supportive of the use of social networks in the workplace.

In his session entitled "Security and Social Networks," Rothke urged organizations to take a more forward-looking, proactive approach to social media use, and encourage their employees to use the services to connect with their customers, clients, and co-workers. "Excessive personal Facebook use is an HR issue, not one for IT or security," Rothke said. "Facebook is very appropriate for Starbucks employees to connect with colleagues and customers, but shouldn't be something that the U.S. Marine Corp should support, for obvious reasons."

The rise of professional cyber criminals. Organized crime has now taken hold in the world of information security threats. So-called script-kiddies used to be more of a nuisance than a real problem, but they've now been replaced by organized networks of cyber-criminals that traffic in passwords, personal identities, and confidential corporate data.

Tom Murphy, Chief Strategy Officer of Bit9, told me that several foreign governments now have large and well-financed cyber-espionage programs. "We came across a problem with an unnamed US agency that had developed an application to track defense assets that was built on top of Google Earth," Murphy said. "Our security tools were flagging Google Earth as an unsafe application—upon further research we discovered that one of the app developers had downloaded files from a site that had been compromised, and the Google Earth application had a number of backdoors and other malware installed."

Leaving the ivory tower. When asked to give some final advice to CIOs about how to approach the pressing IT and security issues of the day, Lieberman urged CIOs to "get out of their ivory towers" and take a hands-on approach to security and managing their IT departments. "CIOs need to be involved in root-cause analysis. They need to take direct responsibility for their security posture, and not delegate that to an analyst. They need to get their hands dirty. If their IT department isn't seeing the big picture or understanding business needs, it's up to IT management to help IT get better, not to punish them. We need CIOs to get involved on both the operational and technical levels. Many CIOs have outsourced work, and protect themselves with contracts. CIOs are often compensated by how low they can drive down IT costs, not how they can transform IT into something good for the business."

Are security topics top of mind for you and your IT staff for 2011? Let me know what you think via email (jjames@windowsitpro.com) or on Twitter (@jeffjames3).

—Jeff James

Exchange Server in the Cloud: Still Cloudy

There was a lot of noise about Google losing users' Gmail data at the end of February. Could the same thing happen in Microsoft's data centers for Exchange Online or Office 365? Both Microsoft and Google, as the two power players of hosted messaging, have had some widely publicized failures in uptime. These are the real fears that keep businesses deploying Microsoft Exchange Server on-premises, where the IT department can control the data.

In the latest poll on the *Windows IT Pro* Exchange & Outlook page, I asked, "How would you describe the makeup of your Exchange Server organization?" Here are the results:

- 50% On-premises, on physical hardware
- 18% On-premises, partly physical, partly virtualized
- 29% On-premises, wholly virtualized
- 1% Partly on-premises, partly in the cloud
- 1% Wholly in the cloud
- 1% Other

Is anybody really surprised by these results? Well, actually, I'm a bit surprised. I mean, I knew not to expect the cloud option to receive a high percentage, but I certainly thought to see more than 1 percent, or 2 percent if you include the hybrid cloud/on-premises possibility.

Microsoft and everyone else continues to talk about the cloud as the great savior for businesses—save money, save hassle, save your soul, apparently, if you just move your IT systems to the cloud. And every time I ask a question to IT pros about what they're actually doing in their environments, the cloud option is a no-show.

Is there a disconnect between what Microsoft and other vendors are pushing and what businesses find they really need?

Is there a disconnect between what Microsoft and other vendors are pushing and what businesses find they really need? Or do businesses resist this change because it's something that's different and seems out of their control? You'll have to tell me. I do think it's worth looking at what the cloud has to offer, even if you ultimately find it doesn't meet the needs of your organization—at least for now. In "Exchange 2010 Architecture: Microsoft's Jon Orton Talks About Exchange Online" (www.windowsitpro.com, InstantDoc ID 129764), Jon Orton lays out some compelling reasons to trust your messaging to Microsoft's cloud. Virtualization wasn't exactly an overnight success, but we can see from the above poll results that many organizations have found a place for it in their Exchange Server environments, helped of course by Microsoft coming through with official support policies. Maybe cloud computing will have its day yet.

What reasons do you have for avoiding moving your messaging systems to the cloud? Or for using virtualization? I'd love to hear how you made your decisions (email bwinstead@windowsitpro.com or tweet @bkwins).

—B. K. Winstead

Why Doesn't PowerShell Do Copy and Paste?

Oh, it does. Just not as easily as you might expect.

When you open PowerShell.exe, you're really launching a very small console application that hosts the actual PowerShell engine. That console is (more or less) the same one used by Cmd.exe and other tools; it isn't "owned" by the PowerShell team. Because so many bits of Windows have dependencies on that console, the PowerShell team can't even really make changes to it.

Fun story: PowerShell 1.0 shipped (in 2006) without support for double-byte character sets. You know, like Asian languages, some European languages, etc. That's because the console app is so old (NT 3.1 anyone?). So in PowerShell 2.0, one of the big reasons the PowerShell team developed their own "graphical host" (the ISE) was to get an environment they could control. One that supported TrueType/OpenType fonts and double-byte character sets.

The ISE supports normal copy and paste operations using Ctrl+C, Ctrl+V, and Ctrl+X. The console app doesn't use those keyboard shortcuts, but if you click the window's control box you still get the good old Edit menu, just like you do in Cmd.exe. So you can copy and paste, but it's a hassle. Actually, the team was able to make some changes so that you can highlight text (using your mouse) at any time, press Enter to copy to the clipboard, and right-click to paste. That's a big improvement over Cmd.exe, at least—but it's definitely not as convenient as what you can do in the ISE.

The bottom line? If you want a more modern, Windows-like experience, use the ISE.

The bottom line? If you want a more modern, Windows-like experience, use the ISE. Or, look into a commercial replacement shell such as PowerShell Plus from Idera. But don't hold your breath for huge improvements to that old text-based console app. As I said, the huge number of dependencies upon it make it a tricky thing to modify, so it's likely to stay more or less the same, more or less forever.

—Don Jones

Why the Atrix 4G Can't Revolutionize Computing...Yet

The Atrix 4G is an exciting new entrant into the smartphone war. In addition to its powerful specs (1GHz dual-core processor, 1GB RAM, 16GB memory), this phone can also plug in to a laptop "shell" and interact with Motorola's webtop application on a full-sized screen. The device can also use a docking station to connect to a desktop PC or to your TV as an entertainment center, giving it four different potential use cases.

It's really quite interesting, and it has the makings of something the tech industry has dreamed about for years: a future where users will use one super powerful mobile device that can be plugged into a computer shell, a TV, your car, etc., and act as the central driver of your technological identity. It's a utopian contrast to our currently fragmented world of phones, computers, tablets, eReaders, mp3 players, DVD/Blu-Ray players, and so on.

There's just one problem: the Atrix isn't ready to achieve this dream, in an enterprise or consumer setting. Why not, you ask? There are a few simple reasons.

The Atrix can't replace a full-featured laptop/desktop. Having the laptop form factor is a huge step, but you're still running a mobile OS, and thus have limited capabilities. Being able to run a desktop version of Firefox is great, but the world just isn't cloudy enough to empower an information worker 24/7 without desktop software. And really, if the Atrix and its laptop shell can't replace your regular laptop or desktop, then it's adding to your gadget collection, not reducing.

Enterprise mobility management isn't quite there. Yes, it's true that software vendors have made huge strides, including remote control, the ability to push apps to mobile devices, and monitoring software that works across a variety of mobile OSs. But as it stands, users are still managed largely via their Windows (or Mac) clients. There are just too many unanswered questions about how these mobile-only identities would fit into the mix.

The Atrix and its peripherals are too expensive. When you add up the math of purchasing a $199 smartphone, a $299 laptop shell, and the full carrier plan, data plan, and $45/month tethering plan, you're spending far more than you would on laptops for your organization. (And about the same cost as purchasing a company smartphone and laptop for users.) This makes it really hard to see how the benefits can outweigh the costs.

There's just one problem: the Atrix isn't ready to achieve this dream, in an enterprise or consumer setting.

(Note: I didn't add the $129 cost for the docking station to use the Atrix with a desktop/TV, since that's not really part of the enterprise equation, but there is also that extra cost, for your awareness.)

In conclusion, the Atrix is no doubt a major innovation, and I bet we'll see huge strides very soon in the development of a "central device" that can power the technology in our lives. It starts in the consumer world with the Atrix, but it will eventually pervade into the enterprise world as well.

So keep an eye on the horizon, and consider the Atrix as a very competent smartphone competitor. Just don't go restructuring your organization to accommodate this brave new world yet. Let me know what you think about the Atrix 4G via email (breinholz@windowsitpro.com) or on Twitter (@breinholz).

—Brian Reinholz

AD INDEX

For detailed information about products in this issue of *Windows IT Pro*, visit the web sites listed below.

VENDOR DIRECTORY

The following vendors or their products are mentioned in this issue of *Windows IT Pro* on the pages listed below.

DIRECTORY OF SERVICES | WINDOWS IT PRO NETWORK

Search our network of sites dedicated to hands-on technical information for IT professionals.
www.windowsitpro.com

Support

Join our discussion forums. Post your questions and get advice from authors, vendors, and other IT professionals.
www.windowsitpro.com/go/forums

News

Check out the current news and information about Microsoft Windows technologies.
www.windowsitpro.com/go/news

EMAIL NEWSLETTERS

Get free news, commentary, and tips delivered automatically to your desktop.

- *asp.netNOW*
- *DevProConnections UPDATE*
- *Exchange & Outlook UPDATE*
- *Security UPDATE*
- *SharePoint Pro UPDATE*
- *SQL Server Magazine UPDATE*
- *Windows IT Pro UPDATE*
- *Windows Tips & Tricks UPDATE*
- *WinInfo Daily UPDATE*

www.windowsitpro.com/email

RELATED PRODUCTS

Custom Reprint Services

Order reprints of *Windows IT Pro* articles. Diane Madzelonka at Diane.madzelonka@penton.com.

Windows IT Pro VIP

Get exclusive access to over 40,000 articles and solutions on CD and via the Web. Includes FREE access to eBooks and archived eLearning events, plus a subscription to either Windows IT Pro or SQL Server Magazine.
www.windowsitpro.com/go/vipsub

SQL SERVER MAGAZINE

Explore the hottest new features of SQL Server, and discover practical tips and tools.
www.sqlmag.com

ASSOCIATED WEBSITES

DevProConnections

Discover up-to-the-minute expert insights, information on development for IT optimization, and solutions-focused articles at DevProConnections.com, where IT pros creatively and proactively drive business value through technology.
www.devproconnections.com

SharePoint Pro

Dive into Microsoft SharePoint content offered in specialized articles, member forums, expert tips, and Web seminars mentored by a community of peers and professionals.
www.sharepointpromag.com

NEW WAYS TO REACH *WINDOWS IT PRO* EDITORS:

LinkedIn: To check out the *Windows IT Pro* group on LinkedIn, sign in on the LinkedIn homepage (www.linkedin.com), select the Search Groups option from the pull-down menu, and use "Windows IT Pro" as your search term.

Facebook: We've created a page on Facebook for *Windows IT Pro*, which you can access at: http://tinyurl.com/d5bquf. Visit our Facebook page to read the latest reader comments, see links to our latest web content, browse our classic cover gallery, and participate in our Facebook discussion board.

Twitter: Visit the *Windows IT Pro* Twitter page at www.twitter.com/windowsitpro.

Windows IT Pro

by Jason Bovberg

Time for BBQ!

PRODUCT OF THE MONTH

Surely the overlap between tech geek and grillmaster is fairly high. Personally, I love geeking out at the BBQ, using all sorts of gadgets to improve the flavor and impact of my grilled foods. Now we have word from iDevices of the world's first wireless cooking thermometer for iPod touch, iPhone, and iPad. It's the iGrill, and it works via a long-range Bluetooth (over 200 feet) and app-enabled connection. It not only lets you gauge temperature, it also shows you remaining cooking time, lets you share and browse recipes, and doubles as a kitchen timer. The iGrill costs $99.99. Check it out at the company website (www.igrillinc.com), where you'll also find a helpful *Countdown to BBQ Season!* timer.

USER MOMENT OF THE MONTH

Back when I worked in an elementary school's administration office, I had multiple duties, including performing the occasional tech acquisition and systems administration. One day, a third-grade teacher came to the office, complaining, "I have the strangest problem—the bottom half of all my printouts are blurry!" I ordered a replacement printer drum and sent her on her way. After replacing the drum, I tested the printer, and all seemed fine. A week later, the teacher returned to the office with some printed sheets in hand. "Same weird problem," she said, showing me. Raising my eyebrow, I asked to accompany her back to her classroom and show me how she prints documents. Sure enough, as each sheet began to emerge from the printer, she would yank it out prematurely. "Yep, there it is again!" she said.

—Steven Albright

Figure 1: Darn, I was so close!

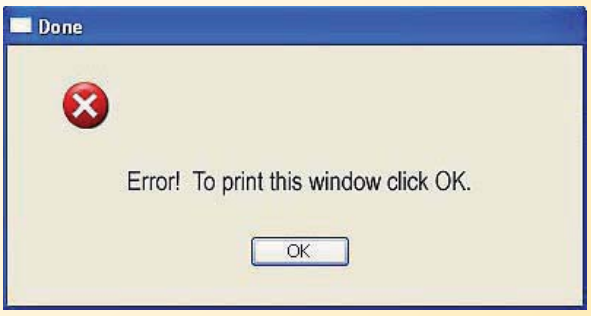


Figure 2: Important hard-copy documentation

May 2011 issue no. 201, *Windows IT Pro* (ISSN 1552-3136) is published monthly. *Windows IT Pro,* 748 Whalers Way, Fort Collins, CO 80525, (800) 793-5697 or (970) 663-4700. Sales and Marketing Offices: 748 Whalers Way, Fort Collins, CO 80525. Advertising rates furnished upon request. Periodicals Class postage paid at Loveland, Colorado, and additional mailing offices. **POSTMASTER: Send address changes to *Windows IT Pro,*** 748 Whalers Way, Fort Collins, CO 80525**. SUBSCRIBERS:** Send all inquiries, payments, and address changes to *Windows IT Pro,* Circulation Department, 748 Whalers Way, Fort Collins, CO 80525. Printed in the USA.

BIG CAPACITY
LOW PRICE

Introducing EMC® VNXe™. Simple and efficient storage starting under $10K.

Visit EMC Booth # 901

EMC²

Microsoft

Now we're talking private cloud, not just virtualization.

Windows Server is changing the conversation.

Windows Server Hyper-V and **System Center** let you manage your infrastructure as a private cloud: a pool of computing resources that lets you allocate computing power to your applications as your business requires. And Microsoft provides common management, identity and development tools that work across your infrastructure. End-to-end control. Agility beyond virtualization.
That's Cloud Power.

Find out more about our private cloud solutions. **Microsoft.com/cloud/privatecloud**

Cloud Power

Windows Server Hyper-V



HIGHLIGHTS & AGENDA

For over **a decade**, IT & DevConnections has partnered with Microsoft to produce the premier IT & developer conferences in the U.S.A. In June 2011, this partnership launches in Europe.

Now Coming to Europe

PAST HIGHLIGHTS OF CONNECTIONS INCLUDE

SHAUN PIERCE, General Manager, Lync Server Division, Microsoft, celebrates the release of Microsoft Lync

SCOTT GUTHRIE, Corporate Vice President, .NET Developer Platform, Microsoft, launch of Silverlight 4

BOB MUGLIA, President, Server and Tools Business, Microsoft, launches Visual Studio 2010

Collaboration between IT & DevConnections and Microsoft continues, bringing great insight for IT professionals like you into how to use the newest technologies. What will you and your team see at IT & DevConnections in 2011? You'll need to sign up and be there to find out!

IT & DevConnections will launch in Germany 8-10 June 2011. Check our website for full session descriptions and to download our expanded brochure and agendas.

Agenda at a Glance

WEDNESDAY, 8 JUNE 2011	
07:30	Registration Opens
09:00 - 12:00	Workshops
12:00 - 13:00	Lunch
13:00 - 16:00	Workshops
THURSDAY, 9 JUNE 2011	
07:00 - 17:00	Conference Registration
08:30 - 09:30	Breakfast & Expo Opening Expo Hall Hours: 08:00-18:00
09:30 - 10:45	Keynote
11:15 - 12:30	Conference Sessions
12:30 - 13:30	Lunch
13:30 - 17:45	Conference Sessions
18:00 - 18:45	Sponsor Sessions
18:45 - 20:00	Special Evening Events
FRIDAY, 10 JUNE 2011	
07:00 - 17:00	Conference Registration
08:30 - 09:30	Breakfast & Expo Opening Expo Hall Hours: 08:00-18:00
09:30 - 10:45	Keynote
11:15 - 12:30	Conference Sessions
12:30 - 13:30	Lunch
13:30 - 17:45	Conference Sessions

Conference Highlights

- **Over 115 Technical Sessions**
- **In-depth Full Day Workshops**
- **Evening Open Spaces Sessions** (attendees choose topics)
- **Networking with Your Peers**
- **Q&A with Microsoft & Industry Experts**
- **Connections Beerfest**
- **Partner Expo**
- **Conference T-shirt and Attendee Bag**
- **A Chance to Win a Mediterranean Cruise**
- **Continental Breakfast & Lunches included**

IT& DevCONNECTIONS
powered by Microsoft®

2011 CONFERENCE | 9-10 JUNE 2011

SUPER EARLY BIRD
Price before 30/04/11: €899 (+VAT)

EARLY BIRD
Price before 13/05/11: €999 (+VAT)

REGULAR PRICE: €1199 (+VAT)



CHECK WEBSITE FOR SESSION & WORKSHOP DESCRIPTIONS, SPEAKER BIOS, AND UPDATES

Workshops

8 June 2011 | 09:00 to 16:00

THE COST OF A WORKSHOP IS IN ADDITION TO THE REGULAR CONFERENCE FEE.
Early bird price €349 +MwSt, register before 13/5/2011.
Regular Price €499.

WINDOWS

WPR01: Don Jones' Windows PowerShell Crash Course
DON JONES

EXCHANGE

EPR01: Microsoft Exchange Server 2010 High Availability and Disaster Recovery Strategies and Best Practices
VLADIMIR MELOSKI

SHAREPOINT ADMIN

HPR01: Dan Holme's SharePoint Collaboration MasterClass
DAN HOLME

SHAREPOINT DEVELOPER

HPR02: Business Connectivity Deep Dive
SCOT HILLIER

SQL SERVER ADMIN

SPR01: SQL Server Performance Tuning from A to Z
KIMBERLY L. TRIPP AND PAUL S. RANDAL

SQL SERVER DEVELOPMENT

SPR02: Windows and SQL Azure Storage Deep Dive (Presented in German)
RAINER STROPEK

VISUAL STUDIO

VPR01: Every Class as a Service – WCF as the New .NET
JUVAL LOWY

ASP.NET

APR01: A Day of ASP.NET MVC
SCOTT ALLEN

SILVERLIGHT

LPR01: Silverlight Development Workshop
JOHN PAPA AND DAN WAHLIN

Sessions

WINDOWS

WIN01: Building Your Own Reusable Tools ("Script Cmdlets") in PowerShell
DON JONES

Have you mastered the basics of running commands interactively in Windows PowerShell? If so, you're really just steps away from turning those commands into reusable, packaged tools that can be shared with colleagues and coworkers. Windows PowerShell author, columnist, and guru Don Jones shows you how to take a complex command and turn it into something that's almost indistinguishable from a PowerShell native cmdlet – all with a minimal amount of scripting, and absolutely no need for Visual Studio. You'll learn the rules of function output, how to build advanced functions, and more in this hard-hitting, example-packed session. All sample scripts are made available for download after the conference, so you'll have templates ready to adapt and use in your own environment.

WIN02: SQL Server Administration for the "Reluctant" DBA
DON JONES

Are you tasked with maintaining one or more SQL Server instances simply because you are your organization's "Microsoft person?" No desire to become a full-time DBA, but need to know what to do with these SQL Server databases? This is the session for you: Join Don Jones, Microsoft TechNet Magazine columnist and self-proclaimed "Jack of All Trades" for this informative session that covers SQL Server operations, monitoring, backup and recovery, high availability, and even performance tuning. You'll learn what to do with indexes – and when to do it. You'll see how SQL Server backups work under the hood, and learn best practices for a backup plan. You'll even learn about various high availability options, and figure out which one is right for you.

WIN03: Preparing Software for Deployment with a Windows 7 Upgrade
GREG SHIELDS

Application Guru Greg Shields hates walking around the office, DVDs in hand. He hates clicking Next, Next, Finish to install software. He also hates dealing with applications that are directly installed into his Windows 7 deployment images. That's why he taught himself software packaging, and automated software installation for a company of thousands. Join Greg in this session to learn his tricks for repackaging software. Then you too can automatically deploy applications with your Windows 7 deployments.

WIN04: Windows Server Core R2: The Low-Maintenance, Small-Footprint Windows You've Been Ignoring
DON JONES

Many administrators gave up on Server Core with Windows Server 2008 for a variety of good reasons – but many of those reasons no longer exist in Windows Server 2008 R2. Learn about changes to Server Core, and learn why smart organizations are adopting it for critical server roles in infrastructure and more. Don Jones busts myths about Server Core – like what software really can and cannot run on it – and helps you discover unique advantages, such as the fact that it's perhaps the best version of Windows Server to run as a virtual machine guest. You'll separate fact from fiction and hype from reality, discover if Server Core has a place in your organization, and even learn some hidden tips and tricks for managing it more easily and effectively.

WIN05: 10 Steps to Solving Almost Any vSphere Performance Problem
GREG SHIELDS

Virtualization Expert Greg Shields likes to talk about "the network interface problem that is really a processor performance problem." That's because with virtualization, our typical troubleshooting gut feelings get thrown out the window. As a result, solving performance problems can't occur by gut instinct alone. You need a structured approach. Get that approach with Connections' Performance Master Greg Shields. He'll explain the exact steps to track down any VMware performance problem.

WIN06: The Best Free Tools for Windows Desktop Administration
GREG SHIELDS

Getting tools and solutions to solve the daily problems in IT just keeps getting harder. That's why you've got to look to free solutions to get the job done. Master Toolsmith Greg Shields is a collector of just those tools. In this fun and exciting session, he'll share the tools in his quiver along with a few humorous stories about how they've saved the day in his IT career. Considered the must-see session at WinConnections, join Greg to laugh a little, learn a little, and leave with more free stuff than in any conference goodie bag.

WIN07: HTML5 + Internet Explorer 9 = No Buzzword Bingo! (German)
DARIUSZ PARYS

Internet Explorer 9 adds new support for HTML5, CSS3, and many other new web standards. We'll take a dive into the work the engineering team at Microsoft has done to make the browser faster through its new JavaScript engine, the work they've done to ensure that the same mark-up works across all browsers and how hardware acceleration will make your site run faster, without any changes to your code! This demo heavy session will help you understand the value of HTML5 and Internet Explorer 9, and what new opportunities they open for the web.

WIN08: Managing Enterprise Scale Hyper-V Clusters
GUIDO GRILLENMEIER

This is a session that does NOT compare the features of Hyper-V to those of ESX. It also does NOT compare the performance of Hyper-V to that of other hypervisors. We know they all have their differences, but Hyper-V is certainly an attractive option.

This session concentrates on the challenges of actually operating a Hyper-V implementation at enterprise scale in production for more than two years already and how we solved them. What is it like to handle more than 100 Hyper-V servers forming more than 15 clusters across the globe, hosting more than 1000 server VMs? Details that this session covers include best practices for deploying Hyper-V in a cluster, incl. various little traps that you can avoid falling into. Similarly System Center Virtual Machine Manager (SCVMM) brings along its own challenges when planning to leverage it in a global Hyper-V deployment. This includes handling of networks in a cluster and deployment of multiple disks per VM. The session is a result from production use of Hyper-V and not from running it in Test-Labs.

EXCHANGE

EXC01: Notes from the Field: Best Practice for Exchange 2010 (German)
SIEGFRIED JAGOTT

Learn what I learned about Exchange Server 2010 SP1 from putting together the best-selling book on Exchange: Microsoft Press' Exchange 2010 Best Practices. This session will be about Exchange 2010 optimization, not about how to configure something. We will have discussions about what makes sense to configure in Exchange 2010 and why, but also when you should not consider it. Learn from the best practices on configuring and managing Exchange from the industry's top experts from the Exchange TAP program including these areas: General areas such as namespace planning, Hub Transport servers and message routing, CAS planning and implementation, Mailbox including DAG design and some of the areas that are not so often touched: Unified Messaging.

EXC02: Common Mistakes in Deploying Exchange 2010 (German)
FRANK CARIUS

Get some deep insights about common mistakes in installing and configuring Exchange and associated components. It looks easy to setup a new Exchange Server but there are hundreds of things, that can go wrong. Some are easy to find, others can cost you hours. Or have you ever heard about AdminSDHolder, incorrect smarthost configurations or the right way to allow Exchange to act as relay? Even a mixed environment can drive you crazy with empty admingroups, wrong management tools and the recipient update service. So finding and fixing bugs is a great (but sometimes expensive) way to learn more about the internals and concepts of exchange. Prevent some common problems and learn about the logic behind.

EXC03: Creating Effective Strategies for Exchange 2010 Backup and Restore
VLADIMIR MELOSKI

Microsoft Exchange Server 2010 brings great new set of storage technologies. Did you know that deploying Exchange Server 2010 will bring companies greatly reduced cost and still fast, reliable and high availability Exchange?

Are you interested in learning how to develop backup/restore strategy that best fits your needs? Do you make backups using Exchange Native Data Protection?

In this session you will find out how Microsoft Exchange Server 2010 technologies have pushed the limits towards lowering expenses and increasing options for high availability and data protection scenarios.

EXC04: Exchange 2010 Tips and Techniques (German)
DEJAN FORO

Microsoft Exchange Server 2010 brings great new set of storage technologies. Did you know that deploying Exchange Server 2010 will bring companies greatly reduced cost and still fast, reliable and high availability Exchange?

Are you interested in learning how to develop backup/restore strategy that best fits your needs? Do you make backups using Exchange Native Data Protection?

In this session you will find out how Microsoft Exchange Server 2010 technologies have pushed the limits towards lowering expenses and increasing options for high availability and data protection scenarios.

EXC05: Monitoring Your Exchange 2010 Organization with SCOM
VLADIMIR MELOSKI

Microsoft Exchange Server is a business-critical system for many organizations. In this session, you will learn how to respond to challenges of proactively monitoring your Exchange organization to lower costs on support and diagnostics.

Several scenarios will be presented on how Exchange Server Management pack for System Center Operations Manager provides you with detailed and centralized information on health state, performance, service dependencies, and topology views and detailed reporting. You will also learn how to customize some of the Management Pack components in order to configure the best monitoring information that meets your company's business requirements.

EXC06:Client Access Servers – A Closer Look
SIEGFRIED JAGOTT

This session looks at the CAS role in Exchange 2010 in detail. In particular we explore the role and why it's more important now that it ever has been.

We focus on obtaining certificates and binding them to a CAS server, and step that up to building a CAS array, and how that integrates into our High Availability design in conjunction with DAG's for the mailbox role.



EXC07: Integrating Lync Server 2010 and Unified Messaging (German)
DESMOND LEE

Lync Server 2010 is the latest generation of unified communications platform which powers the communications and collaborative landscape to the next level. Be it on the deskop, laptop or mobile devices, a solid understanding of multiple technological disciplines in the back-end is indispensable for a successful deployment. From Active Directory, Public Key Infrastructure, Exchange/Outlook to integration with third party devices, this session highlights the "must-know" and troubleshooting tips and tricks to help ease your Lync rollout and support pains.

EXC08: Signing and Encryption - DE-Mail, ePost, and S/MIME (German)
FRANK CARIUS

Many companies are using emails instead of mail and fax to save money and to speed up processes and increase customer satisfaction. But how can the recipient be sure, that the sender is the real sender? Spoofing and spam are real and false positives can also block your business. SMIME is one way to make sure, that you are the sender. The German government started an initiative to offer a secure and trustworthy messaging infrastructure called De-Mail. Learn how it works technically and how you can connect your company to it. The German post started a competitive system called ePost. How does that work? But don't forget, that PGP and SMIME have been here for many years and are easy to use. Learn about solutions for companies. Expect technical and logical answers but I'm not a lawyer.

ASP.NET

ASP01: Using jQuery Templates with ASP.NET
STEPHEN WALTHER

ASP02: ASP.NET + OData + jQuery = Goodness
STEPHEN WALTHER

ASP03: ASP.NET Database Development using EF4 and Code-First
PAUL LITWIN

ASP04: Building HTML 5 Applications with ASP.NET Web Forms
STEPHEN WALTHER

ASP05: The Scaling Habits of ASP.NET Applications
RICHARD CAMPBELL

ASP06: A WebForms Programmer's First ASP.NET MVC 3 Application
PAUL LITWIN

ASP07: TDD with ASP.NET MVC
SCOTT ALLEN

ASP08: Chart Your Success using the Microsoft Chart Control
PAUL LITWIN

ASP09: Razor Sharp Views in ASP.NET MVC
SCOTT ALLEN

ASP10: Why Web Performance Matters
RICHARD CAMPBELL

ASP11: LINQ in Layered Architectures
SCOTT ALLEN

ASP12: Enter the Web Matrix (German)
CHRISTIAN WENZ

ASP13: Web Application Security with ASP.NET (German)
CHRISTIAN WENZ

ASP14: Accelerate AJAX Applications (German)
CHRISTIAN WENZ

ASP15: Design Considerations for ASP.NET MVC Applications
DINO ESPOSITO

ASP16: ASP.NET MVC3: Unleash the Power of Action Filters
DINO ESPOSITO

SILVERLIGHT

SIL01: Developing for the Windows Phone 7
LAURENT BUGNION

SIL02: Modular Application Development with the MVVM Light Toolkit
LAURENT BUGNION

SIL03: Getting Started with Silverlight
DAN WAHLIN

SIL04: Applying Silverlight's New Features
JOHN PAPA

SIL05: Building Architecturally Sound Silverlight Applications using MVVM, Part 1
DAN WAHLIN

SIL06: Building Sound Silverlight and Windows Phone 7 Applications with MVVM, Part 2
JOHN PAPA

SIL07: Using WCF RIA Services in Silverlight Applications
DAN WAHLIN

SIL08: 0-60 with Silverlight and Windows Phone: Top Tips for Building a WP7 / Silverlight App
JOHN PAPA

SESSIONS AND SPEAKERS ARE SUBJECT TO CHANGE.
SEE WEBSITE FOR UPDATES.
WWW.DEVCONNECTIONS.COM/GERMANY

SHAREPOINT

HAD01: Wish I'd Have Known That Sooner! SharePoint Insanity Demystified
DAN HOLME

After years of helping organizations around the world to deploy and implement SharePoint, Dan Holme has found that there are certain pain points that almost everyone encounters. Some are confusing concepts. Some are bad decisions driven by Microsoft's UI and documentation. Some are due to unnecessarily complex terminology. And some because there are things that SharePoint should do, but can't. In this session, Dan will share the most common and problematic scenarios, and their solutions, with the goal of saving you pain, time, and money. Think of this session as "Lessons Learned," "Best Practices," or "From the Field" on steroids. Whether you're new to SharePoint or a seasoned veteran, in this grab-bag session there will be treasures for you!

HAD02: Designing Governance: How Information Management and Security Must Drive Your Design
DAN HOLME

You've read the white papers, you've "Binged" governance, but how, exactly, do you design a SharePoint implementation that will support governance, security, and information management? Join SharePoint MVP and consultant Dan Holme for a practical, nuts-and-bolts look at the close relationship between your information management requirements and SharePoint's manageability controls, and the demands that relationship places on your design and infrastructure. This session is focused on architecting a logical design of SharePoint that effectively supports your information management requirements and governance plan–the "technical" side of governance. You will learn how to align your governance requirements with SharePoint farms, Web applications, and site collections. You'll discover why some third-party applications are a "design poison pill" and what SharePoint 2010 offers to greatly improve the deployment of a governable design. Gain a deeper understanding of the intricacies and challenges of designing the logical structure of SharePoint, and take away practical, blueprint-like guidance to what a governed SharePoint implementation might look like in your enterprise.

HAD03: A Practical Jump Start to Administering SharePoint with Windows PowerShell
DAN HOLME

Windows PowerShell is the preferred tool for administering and automating SharePoint outside of Central Administration and only with PowerShell can you perform scripted configuration and certain tasks such as granular restore. So if you've been holding back on learning PowerShell, the time has come to tackle it. Join SharePoint MVP Dan Holme for a very practical, super-clear PowerShell jump start. You'll learn that you don't need to be a scripting guru to use and understand PowerShell and you'll learn how easy it is to manage SharePoint with PowerShell.

HAD04: This is me; Is that you? Identity Management in SharePoint 2010
RICHARD TAYLOR

Securing and managing access to resources in SharePoint for your internal users is one thing, but what is the best way to do it for your partners who need access to shared resources? Come to this session to understand a complex problem space and the best ways to manage it. This session will be 50 percent demonstration.

HAD05: Using the New Business Connectivity Services (BCS) to Build Business Solutions
RICHARD TAYLOR

The evolution of the Business Data Catalog is a key feature of SharePoint 2010. In this session Rick will discuss the new improvements to this rich capability. BCS now enables you to bring external database or web services data into SharePoint and the Office System, interact with it, and empower end-users to gain insight into the underlying data in a reusable way. Building end-to-end business solutions has never been easier!!!

HAD06: The 10 Immutable Laws of SharePoint Security
RICHARD TAYLOR

"Thou Shalt secure the entire stack from Level 1 to 7", you will see there is more to securing SharePoint than permissions and locking down IIS. Come to this session to learn Defense-In-Depth of properly securing SharePoint using the OSI model as your guide.

HAD07: Automating Business Processes Using InfoPath 2010 Forms with Integrated SharePoint Designer 2010 Workflows
ASIF REHMANI

Forms and Workflows are essential to business processes. Companies usually rely on programmers to create the forms and workflows using code. Not any more! If you have access to Microsoft InfoPath 2010 and Microsoft SharePoint Designer 2010, you can create powerful data-driven form solutions on your SharePoint sites. InfoPath gives you the ability to pull data from databases and lists, and create forms with data validation and conditional formatting. SharePoint Designer's workflows let you then design powerful multi-step workflows centered around the form collected data. In this session, you see how to design a robust form using InfoPath and then design a workflow using SharePoint Designer to route this form appropriately.

HAD08: Using InfoPath 2010 and SharePoint Designer 2010 to Manage SharePoint List Forms
ASIF REHMANI

SharePoint Designer has been a great tool to customize SharePoint list forms for a long time. Now in SharePoint 2010, you can use InfoPath 2010 to customize the forms as well. What's the difference? Why should you use one tool over the other for this purpose? This session shows how each functionality works and explores the pros and cons of using each method to customize your SharePoint list forms.

HAD09: Use Data Views to Get to Your Data – Both Inside and Outside of SharePoint
ASIF REHMANI

You can use SharePoint Designer to make connections to and present data from internal and external data sources such as SharePoint lists, libraries, xml files, databases and Web services. The focus of this session is on exposing the data to the user using the XSLT Web Parts. These Web Parts can be manipulated in a variety of ways to present the information to the end user. In this session, you'll see how the list view and data view tools can be used to reformat the presentation of the data using conditional formatting, pre-formatted styles, xPath expressions and more.

HAD10: Manage Your External Data Using Business Connectivity Services – without Code
ASIF REHMANI

The Business Connectivity Services (BCS) is an evolution of the concept of Business Data Catalog (BDC) that was introduced in SharePoint 2007 to get access to your line of business data. In addition to consuming your data, BCS lets you also write back data to your external systems. SharePoint Designer 2010 is used to define your connection properties by creating External Content Types (ECT) without the need for programming! In this session, you see how you can surface this data using external lists, metadata in SharePoint lists and also your Outlook application to create robust business solutions.

HAD11: Office 365: An Overview (German)
STEFFEN KRAUSE

The deployment, configuration and maintenance of a collaboration infrastructure that consists of mail, workspaces and real-time communication today requires a high level of knowledge, experience and work. With Office365 you can now just rent these services and make them available to your end-users without installing them. This session gives an overview of Office365 features, deployment and administration.

HAD12: Organizing Enterprise Documents in SharePoint 2010
AGNES MOLNAR

In SharePoint 2010, documents can be organized not only into document libraries and folders, but also into Document Sets that provide us the capability of managing, editing and downloading documents in a set, can share metadata and version numbers, moreover we can initiate workflows for the whole document set.

This session will focus on the organizing and management of documents in document libraries, folders and document sets – including metadata management, Content Types, Content Organizer Rules, Enterprise Search, etc.

HAD13: Information Architecture and Enterprise Search: Better Together
AGNES MOLNAR

Planning your Information Architecture is one of the most important factors that's required for a successful deployment: well-organized documents and items, metadata management, Content Types, Workflows, etc. are what are you need to be familiar with. The more content you have, the more important is a well-planned and well-organized Information Architecture.

But storing the information is not enough. You also need to find the stored items and to use them in an efficient way. Enterprise Search is indispensable in this story: it is the part of your Information Architecture and completes it at the same time.

This session will demonstrate the relationship between these two as well as will demonstrate some best practices in order to help you to achieve a better and more optimal Information Architecture – integrated with Enterprise Search, all based on SharePoint.

HAD14: Implementing Enterprise Search in SharePoint 2010
AGNES MOLNAR

SharePoint 2010 Enterprise Search, especially with the features of the integrated FAST Search is better and more powerful than ever before. Because of the various versions and wide range of functionality, first we have to build and understand the comparison matrix of SharePoint 2010 Search. After that, I'll demonstrate a lot of best practices for building and administering an effective search infrastructure, including SharePoint 2010 Search Engine, FAST Search Server 2010 for SharePoint, search federation, metadata management serving the effective search and information architecture investments.

HAD15: Information Architecture and the Managed Metadata Service: A to Z
DAN HOLME

Join SharePoint MVP Dan Holme for a down-and-dirty, deep examination of the configuration and management of the Managed Metadata Service, and what the MMS does to support your enterprise information architecture. You'll explore every nook and cranny of this powerful service application, and see how to provide both centrally managed taxonomy and user-driven folksonomy for enterprise tags. You'll also explore content type syndication and best-practice guidance for topologies to support your information architecture.

HDV01: Creating Search-Based Solutions with SharePoint 2010
SCOT HILLIER

Search-based solutions are applications that use a search page as the primary interface. Solutions such as image searching or travel searching in Bing are good examples of search-based solutions. SharePoint 2010 offers developers new ways to extend search and create search-based solutions. In this session, attendees will learn to create search-based solutions by using custom relevance models, extending SharePoint 2010 search parts, and utilizing .NET Assembly Connectors to access external systems. The techniques presented will prepare attendees to create search-based solutions on their own.

HDV02: Advanced External Lists in SharePoint 2010
SCOT HILLIER

External Lists allow data from External Systems to appear as lists in SharePoint 2010. External Lists, however, do not have all of the capabilities of standard lists and database tables. This session will present the differences, limitations, and workarounds that allow you to get the most out of External Lists. The differences between standard SharePoint lists and External Lists will be presented first along with strategies and workarounds for limitations such as attachments and workflow support. Then, the differences between database tables and External Lists will be presented along with strategies and workarounds for limitations such as attachments, folders, and versions. Attendees will exit the session with new ideas for implementing External Lists in their SharePoint 2010 solutions.

HDV03: Using Outlook and the SharePoint Workspace with SharePoint 2010
SCOT HILLIER

SharePoint 2010 provides powerful ways to use data offline through Outlook 2010 and the SharePoint Workspace. In this session, you'll learn how to synchronize sites, lists, and libraries with Outlook and the SharePoint Workspace. You'll learn how data is installed and managed on the client so that you can understand the proper way to work with offline data. You'll learn limitations and workarounds associated with offline data including conflict resolution and collaborative document creation. Attendees will exit this session with a complete understanding of how offline data is synchronized, managed, and utilized in Office clients.

HDV04: Making Your Solutions Pop with Fluent UI Extensibility
WOUTER VAN VUGT

For a developer it is the tip of the iceberg, but for your users it is the iceberg itself. The key ingredient for building fantastic applications on the SharePoint platform is an intuitive and well integrated user interface. It is that little bit of code that unlocks the entire solution.

In this session you will learn about the new ways you can extend the SharePoint 2010 Fluent Interface. Come learn how you can code against the Ribbon using dynamic page components. Experience the benefits of the new client side object model to provide rich interaction with the user. Show modal dialogs, status bar messages and other notifications. You will leave the session ready to make that little tip of the iceberg pop and give your application the edge it deserves.

HDV05: Coding Against the New Office Service Applications
WOUTER VAN VUGT

SharePoint 2010 has many new service applications that you can make use of. One key service application is Word Automation Services which allows you automate an entire document process; from inception to print.

Learn how to build advanced document solutions on top of this service application and learn how to combine the powers of Word with the other Office service apps.

HDV06: Building Service Applications for SharePoint 2010
WOUTER VAN VUGT

This session will discuss why every SharePoint 2010 developer can and should build Service Applications. We'll debunk the idea that writing Service Applications is hard and demo how everybody can and should build them as part of their SharePoint 2010 solution. We also show you how to migrate your existing web services or services applications to the SharePoint 2010 Service Applications model. This session will be about architecture and writing code!




SHAREPOINT & SQL SESSIONS

Enter to WIN!

Enter the contest in the Expo Hall to

WIN a 1-week Mediterranean cruise for two!

To win, you must be present in the Expo Hall at the time of the draw

HDV07: Ease the Development Process with Visual Studio 2010 SharePoint Developer Tools (German)
REINER GANSER

Die VS 2010 SharePoint Deveoper Tools bieten eine integrierte Umgebung für die Entwicklung von SharePoint 2010 Lösungen. Diese Session gibt einen Überblick über diese Tools, die mit Visual Studio 2010 ausgeliefert werden. Inhalte dieser Session sind der Überblick und Demonstration der Projekt- und Element-Vorlagen, die verschiedenen Designer und Wizzards, Packaging, Application Life Cycle Management und sonstige Erweiterungen.

HDV08: SharePoint 2010 Version Comparison (German)
REINER GANSER

SharePoint gibt es in vielen Versionen (kostenlose Foundation, SharePoint Server 2010 Standard und Enterprise), und dann stehen noch Erweiterungen wie der Search Server (Express und 2010) zur Verfügung. In dieser Session erhalten Sie anhand von Beispielen einen Überblick, wo die Unterschiede liegen und welche Funktionen in den einzelnen Versionen inkludiert sind (z.B. Formulare, BCS). Zusätzlich werden Kombinationsmöglichkeiten gezeigt (z.B. Search Server und Foundation).

HDV09: Developing SharePoint 2010 Workflows with Visual Studio 2010 (German)
REINER GANSER

SharePoint 2010 enthält viele neue Workflow Funktionen und viele Erweiterungen in den Tools für die Erstellung von Workflows. SharePoint Designer 2010 hat einen neuen Workflow Designer für die Erstellung von Workflows. Diese können direkt nach Visual Studio exportiert werden. Visual Studio 2010 wiederrum hat etliche Erweiterungen erfahren mit einem neuen Workflow Designer, Unterstützung für Workflow Aktivitäten in einer Sandbox, sowie den neuen SharePoint Tools Packaging Designer. Nicht zuletzt spielt auch Visio eine gewichtigere Rolle bei der Erstellung von Workflows. Diese Session beschreibt und demonstriert die neuen Funktionen.

HDV10: Building Your First Windows Phone 7 Application for SharePoint 2010
PAUL STUBBS

Take your SharePoint business applications on the go with Windows Phone 7. Windows Phone 7 has great integration with SharePoint via the Office hub, but how do access your custom line of business applications on the phone? In this session you will learn how to build your first Windows Phone application for SharePoint. Learn the fundamentals that will give you a running start for your own applications.

HDV11: Integrating SharePoint and Windows Azure
STEVE FOX

Increasingly, developers are building applications that live in the cloud. One of Microsoft's key strategies for the cloud is Windows Azure. Using SharePoint, you can build cloud-based solutions that can help offset data storage costs by using BLOB storage, expand your reach of service capabilities through more widely deployed WCF services, and increase your surface area for devices and platform. If you're interested in better understanding how SharePoint and Windows Azure can come together, than you can't miss this session.

HDV12: Exploring the Developer Story for Office 365
STEVE FOX

Abstract not available.

HDV13: Advanced SharePoint Data Access with Silverlight
PAUL STUBBS

SharePoint and Silverlight make an unbeatable combination for building great web applications. In this session, you will learn how to develop these solutions more easily than ever with Visual Studio 2010 and SharePoint's client object model, WCF Data services, and Web Services. You will see how to access data from SharePoint using Silverlight, such as how to deal with large datasets, out-of-browser support, piggybacking data on the web page, external data access, uploading document, creating Wiki pages and more. So if you are tired of slides be sure to come to this fast-paced, demo-only session.

SQL SERVER

SQL01: SQL Server Mythbusters
PAUL RANDAL

SQL02: SQL Server Corruption Survival Techniques
PAUL RANDAL

SQL03: SQL Server – Optimizing Procedural Code
KIMBERLY L. TRIPP

SQL04: SQL Server Covering: Concepts, Concerns and Costs
KIMBERLY L. TRIPP

SQL05: SQL Server Filtered Indexes and Filtered Stats
KIMBERLY L. TRIPP

SQL06: SQL Server Index Fragmentation – The Hidden Menace
PAUL RANDAL

SQL07: How to Optimize TEMPDB Performance
BRAD MCGEHEE

SQL08: Inside the SQL Server Transaction Log
BRAD MCGEHEE

SQL09: Hasta la Vista Baby, The Resource Governor has Spoken
BODO MICHAEL DANITZ

SQL10: Finding Your Way Through the DMV Jungle
BODO MICHAEL DANITZ

SQL11: Using a Database Without Installing It – SQL Azure and SQL Azure Reporting (German)
STEFFEN KRAUSE

SQL12: Taking SQL Server Beyond Relational into the Realm of Unstructured Data Management
MICHAEL RYS

SQL13: Designing Reports in SQL Server 2008 R2
PAUL LITWIN

SQL14: Introduction to SQL Server "code named" Denali
GOPAL ASHOK

SQL15: SQL Server Denali AlwaysOn: The Next Generation High Availability Solution
GOPAL ASHOK

SQL16: Taking SQL Server into the Realm of Spatial Data Management
MICHAEL RYS

VISUAL STUDIO

VS01: Introducing the Azure AppFabric Service Bus
JUVAL LOWY

VS02: A Modular Approach to Development Process
JUVAL LOWY

VS03: Discover a New WCF with Discovery
JUVAL LOWY

VS04: .NET 4.0 und C# 4.0 (German)
BERND MARQUARDT

VS05: Parallel Programming with .NET 4.0 (German)
BERND MARQUARDT

VS06: Creating Advanced Touch Interfaces in WPF
BILLY HOLLIS

VS07: Advanced Features of WPF
BILLY HOLLIS

VS08: LightSwitch! What is it and why do we need it? (German)
TOM WENDEL

VS09: 10 Crazy Things You Can Do with Expression Blend (German)
OLIVER SCHEER

VS10: Three Screens and a Cloud – A Social Media App for Multi Screens (German)
OLIVER SCHEER

VS11: Sharpening UI Design Skills: A Path for Developers
BILLY HOLLIS

VS12: Business Apps In Half the Time: WPF and Silverlight Styling (German)
MARKUS EGGER

VS13: A Graphics Design Lesson for Developers (German)
MARKUS EGGER

VS14: Using Services and SOA for More Versatile and More Maintainable Applications
MARKUS EGGER

VS15: Modern Visual Basic Programming – What Visual Basic Developers Really Have to Know About .NET 4.0 (German)
PETER MONADJEMI

VS16: Automating Build, Test and Lab with Visual Studio 2010 (German)
NENO LOJE

VS17: Visual Studio 2010 – Feature Highlights for Developers (German)
NENO LOJE

VS18: Code Correctness and Software Tools for .NET 4 Developers
DINO ESPOSITO

VS19: 10 Things You Can Do To Use Windows Azure More Effectively
RAINER STROPEK

VS20: Zen of Architecture
JUVAL LOWY

SPONSOR01: Visual Studio Ultimate: You Love It – We Tell You How to Convince Your Management to Pay for It
STEFFEN RITTER

SPONSOR02: Microsoft's Great Infrastructure for Game Developers
TOM WENDEL

SESSIONS AND SPEAKERS ARE SUBJECT TO CHANGE.
SEE WEBSITE FOR UPDATES.
WWW.DEVCONNECTIONS.COM/GERMANY

THE CONVERSATION BEGINS HERE

QUESTIONS ANSWERED • STRATEGY DEFINED • RELATIONSHIPS BUILT

9-10 June 2011

8 June
Pre Conference Workshops

KARLSRUHE, GERMANY

SOME OF OUR SPEAKERS

DAN HOLME
Intelliem, Inc.

STEPHEN WALTHER
Superexpert

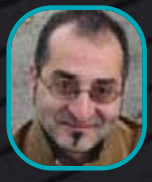
RAINER STROPEK
software architects og

SCOTT ALLEN
Pluralsight

STEVE FOX
MIcrosoft

SCOTT GUTHRIE
MIcrosoft

DAVE MENDLEN
MIcrosoft



DINO ESPOSITO
IDesign Inc.

SCOT HILLIER
Scot Hillier Technical Solutions, LLC.

STEFFEN KRAUSE
Microsoft Deutschland GmbH

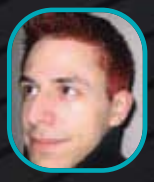
PETER MONADJEMI
activetraining

JOHN PAPA
MIcrosoft

PAUL S. RANDAL
SQLskills.com

KIMBERLY L. TRIPP
SQLskills.com

CHRISTIAN WENZ
Arrabiata Solutions GmbH



TOM WENDEL
MIcrosoft Deutschland GmbH

BERND MARQUARDT
www.go-sky.de

RICHARD CAMPBELL
Strangeloop Networks

MARKUS EGGER
EPS Software

DEJAN FORO
Infosistem

REINER GANSER
Ganser IT-Consulting

BILLY HOLLIS
DotNet Masters

OLIVER SCHEER
MIcrosoft Deutschland GmbH

ASIF REHMANI
Sharepoint e-learning.com

SIEGFRIED JAGOTT
Siemens

DESMOND LEE
Swiss IT Pro User Group

NENO LOJE
teamsystempro.com

VLADIMIR MELOSKI
Semos

STEFEN RITTER
MIcrosoft Deutschland GmbH

RICHARD TAYLOR
Perficient

BRAD MCGEHEE
Red Gate Software

GUIDO GRILLENMEIER
HP

LAURENT BUGNION
IdentityMine

PAUL STUBBS
Microsoft

JUVAL LOWEY
IDesign, Inc.

WOUTER VAN VUGT
code-counsel
Microsoft MVP

TONY REDMOND
Tony Redmond & Associates

AGNES MOLNAR
BA Insight

CHECK WEBSITE FOR SESSION & WORKSHOP DESCRIPTIONS, SPEAKER BIOS, AND UPDATES

Register Today! Call +44 (0)161 929 2800 | **www.DevConnections.com/Germany**